Prikazi in analize

Kibernetsko kartiranje kot orodje za spremljanje kibernetskega tveganja

Avtor: Borut Poljšak

Oktober 2024

BANKA SLOVENIJE
EVROSISTEM

Zbirka: Prikazi in analize

Naslov: Kibernetsko kartiranje kot orodje za spremljanje kibernetskega tveganja

Številka: Oktober 2024

Leto: 2024

Kraj: Ljubljana

Izdajatelj:
Banka Slovenije
Slovenska 35, 1505 Ljubljana, Slovenija
www.bsi.si

Elektronska izdaja/Electronic edition:

https://www.bsi.si/publikacije/raziskave-in-analize/prikazi-in-analize

This publication is also available in English.

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID **212586755**
ISBN 978-961-7230-03-1 (PDF)

Kazalo

Povzetek

Kibernetsko kartiranje omogoča identifikacijo sistemskih vozlišč v sistemu prek spremljanja in analize ključnih tehnologij, storitev in povezav med institucijami finančnega sektorja, ponudniki storitev in sistemi tretjih oseb. Orodje je namenjeno tako mikrobonitetnemu kot tudi makrobonitetnemu nadzoru finančnega sistema. V prispevku je na kratko predstavljena metodologija in aplikativna uporaba orodja za spremljanje kibernetskega tveganja. Orodje omogoča tudi napoved medsebojnih operativnih in finančnih povezav različnih subjektov na bančnem trgu.

Z vidika zagotavljanja finančne stabilnosti je ključno, da imamo nadzorniki finančne sistema pregled nad ključnimi finančnimi in kibernetskimi povezavami na bančnem trgu. Orodje za kibernetsko kartiranje omogoča dodaten vpogled v možne kanale širjenja okužbe in koncentracije tveganja v bančnem sistemu. Kibernetsko omrežje je mogoče obravnavati kot virtualno plast finančnega omrežja, ki jo sestavljajo vse komponente IKT, ki jih finančne institucije uporabljajo pri svojem poslovanju. S kartiranjem finančnega omrežja (tj. finančnega sistema) na kibernetsko omrežje lahko ugotavljamo povezave med tretjimi ponudniki IKT, ki jih uporabljajo finančne institucije.

Ključne besede: kibernetska varnost, kibernetski napad, kibernetski incident, odpornost, sistemsko tveganje, finančno omrežje, kibernetsko omrežje, finančna stabilnost, operativno tveganje, kibernetsko kartiranje

Abstract

Cyber mapping enables the identification of system nodes in the system by monitoring and analysing key technologies, services and links between financial sector institutions, service providers and third party systems. The tool is designed for both micro-prudential and macro-prudential supervision of the financial system. The methodology and the applied use of the tool in cyber risk monitoring are also briefly presented. The tool also allows for the prediction of the operational and financial inter-linkages between different entities in the banking market.

To ensure financial stability, it is essential to have an overview of the key financial and cyber links in the banking market. The Cyber Toolkit provides additional insight into the possible channels of contagion and concentration of risk in the banking system. The cyber network can be considered as a virtual layer of the financial network, consisting of all the ICT components used by financial institutions in their operations. By mapping the financial network (i.e. the financial system) onto the cyber network, we can identify the links between third-party ICT providers used by financial institutions.

Key words: cyber security, cyber attack, cyber incident, resilience, systemic risk, financial network, cyber network, financial stability, operational risk, cyber mapping

1 Uvod

Kibernetsko tveganje lahko opredelimo kot kombinacijo verjetnosti kibernetskih incidentov in njihovega potencialnega vpliva na poslovanje bank, ki se lahko realizira v obliki operativnih prekinitev, finančne škode ali pa prenosa tveganja na ostale sektorje (Poljšak, 2024a). Zato je pomembno, da nadzorniki bančnega sektorja razpolagamo z orodji za spremljanje kibernetskega tveganja. V pristojnosti makrobonitetne politike je spremljanje in blaženje sistemskih kibernetskih dogodkov, ki lahko ogrožajo operativno in finančno stabilnost sistema. S pomočjo kibernetskega kartiranja hitreje in bolj učinkovito spremljamo sistemsko kibernetsko tveganje. V prispevku so predstavljene ključne funkcionalnosti orodja za kibernetsko kartiranje, ki je namenjeno spremljanju kibernetskega tveganja na nivoju bančnega oziroma finančnega sistema. Orodje omogoča pregled medsebojnih operativnih in finančnih povezav različnih subjektov na bančnem trgu. Ključna značilnost orodja je, da omogoča pregled nad kritično infrastrukturo na nacionalni ravni in zagotavlja lažje upravljanje s sistemskim kibernetskim tveganjem (Kaffenberger in Kopp, 2019). S kibernetskim kartiranjem dobimo pregled nad povezavami med finančnimi institucijami ter drugimi ključnimi subjekti na bančnem trgu. Te informacije se lahko uporabijo tako za spremljanje finančne stabilnosti kot tudi nadzorniških aktivnosti kibernetske varnosti. Trenutno s takim orodjem, ki omogoča spremljanje in identificiranje kibernetskega tveganja na nivoju bančnega sistema, razpolaga omejeno število centralnih bank. Bolj kot je kartiranje podrobno, bolj je drago in časovno zahtevno, to velja predvsem za večje ter bolj kompleksne finančne sisteme.

S pomočjo orodja za kibernetsko kartiranje na bančnem trgu zaznavamo koncentracijo tveganj zaradi neposredne ali posredne izpostavljenosti bank do ključnih ponudnikov IKT storitev. Zaznavamo, da kibernetski incidenti vplivajo tako na neposredno izpostavljenost (poslovni odnosi med različnimi finančnimi institucijami) kot tudi posredno izpostavljenost (medsebojna povezanost različnih informacijskih sistemov ali skupnih ponudnikov storitev in operativnih sistemov). Uspešen kibernetski napad na ključnega ponudnika IKT storitev lahko vpliva na poslovanje bank.

Orodje za kibernetsko kartiranje vsebuje tudi napoved izgleda omrežja v naslednjem letu. Pri napovedi kibernetskega zemljevida se uporablja različne tehnike strojnega učenja, ki so zasnovane za napovedovanje časovnih vrst z več sezonskimi obdobji, ki omogočajo prikaz bodočega finančnega ter kibernetskega omrežja. Na podlagi preteklih dogodkov je možno ustvariti novo kibernetsko bazo podatkov in omrežje ter poiskati ključne povezave v sistemu, ki se bodo lahko pojavile med subjekti bančnega sektorja in ponudniki IKT storitev. Možno je tudi napovedati, kje v bančnem sistemu se bodo zgodili kibernetski incidenti. Vse pridobljene informacije koristijo za nadaljnje spremljanje kibernetskega tveganja na nivoju bančnega sistema (Poljšak, 2024b).

Kibernetsko kartiranje nadzornim organom pomaga opredeliti glavna vozlišča sistemskega pomena in pridobiti vpogled v koncentracijo in tveganje okužbe. Pri uporabi kibernetskega kartiranja je treba najti ravnovesje med granularnostjo in uporabnostjo za spremljanje sistemskega kibernetskega tveganja. Rezultat orodja se kaže v prikazu dveh medsebojno povezanih omrežij, in sicer: finančnega in kibernetskega. Kibernetsko omrežje je mogoče obravnavati kot virtualno plast finančnega omrežja, ki jo sestavljajo vse komponente IKT, ki jih finančne institucije uporabljajo pri svojem poslovanju. S kartiranjem finančnega omrežja (tj. finančnega sistema) na kibernetsko omrežje lahko ugotovimo povezave med tretjimi ponudniki IKT storitev, ki jih uporabljajo finančne institucije. Ta pristop omogoča razkritje skupnih ponudnikov IKT (npr. ponudni-

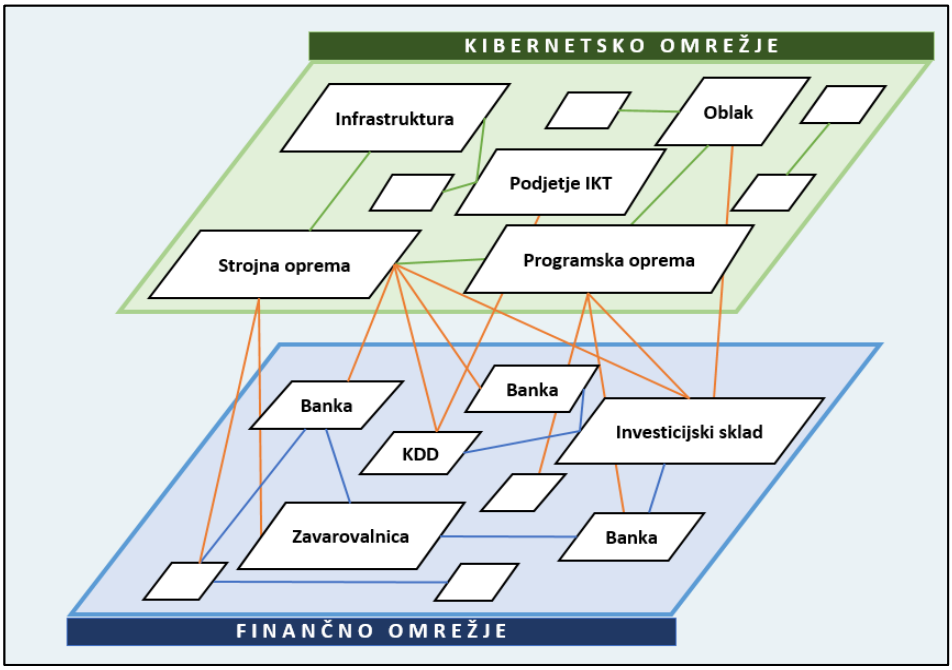
kov storitev v oblaku) v bančnem sektorju. Te informacije omogočajo nadzornikom finančnega sektorja pregled tako nad koncentracijo tveganja v kibernetskem omrežju kot tudi nad kanali prenosa kibernetskega tveganja v finančni sistem (Poljšak, 2024a).

2 Orodje za spremljanje sistemskega kibernetskega tveganja

Na področju spremljanja kibernetskega tveganja je ključno, da nadzorniki razpolagajo z ustreznimi podatki, indikatorji in informacijami, ki se nanašajo na področje kibernetske varnosti (ESRB, 2020a). Sistemsko kibernetsko tveganje, ki se lahko realizira v obliki operativnih prekinitev, finančne škode ali v obliki prenosa okužbe na ostale sektorje, je kombinacija verjetnosti kibernetskih incidentov in njihovega potencialnega vpliva na poslovanje bank (Financial Stability Board, 2018). Ključni sprožilec sistemskega kibernetskega dogodka je kibernetski incident, ki lahko ogrozi kibernetsko varnost informacijskega sistema in krši varnostno politiko finančne institucije (IMF, 2020). Zato je pomembno, da nadzorniki kibernetska tveganja identificirajo in spremljajo tudi s pomočjo orodja kot je kibernetsko kartiranje, ki temelji na mrežnem pristopu (analiza omrežij[1]).

Kibernetsko kartiranje (kvantitativno orodje) vključuje ključne tehnologije, storitve, zunanje ponudnike storitev in njihove povezave z institucijami finančnega sektorja. Na konceptualni ravni je namen kartiranja poudariti ključne finančne in tehnološke povezave med finančnimi institucijami, podjetji ter neodvisnimi ponudniki tehnologij in storitev. S kibernetskim kartiranjem nastane pregled nad finančnimi institucijami in povezavami med finančnimi institucijami ter drugimi kritičnimi subjekti. Za boljše razumevanje ranljivosti in kanalov širjenja okužbe v finančnem sistemu je treba s pomočjo kibernetskega kartiranja opredeliti sistemsko pomembna vozlišča na finančni in operativni ravni, vključno s tretjimi ponudniki (glej sliko 1). Te informacije se lahko uporabijo za nadzor in analizo kibernetskih tveganj za finančno stabilnost (ESRB, 2022).

Slika 1: **Shematični prikaz kibernetskega zemljevida**



Vir: Banka Slovenije

[1] Analiza omrežij je metoda preučevanja odnosov med entitetami v omrežju.

Na sliki 1 so prikazane finančne povezave (na primer obveznosti ali plačilne transakcije) med posameznimi finančnimi subjekti in sektorjem IKT, ki predstavlja kibernetsko omrežje. Kibernetsko omrežje zajema tiste elemente informacijske in komunikacijske tehnologije (IKT, kot so programska in strojna oprema ter ponudniki komunikacijskih storitev), ki predstavljajo osnovno infrastrukturo za vse operativne procese v finančnem omrežju (ECB, 2018 in 2021). Kibernetski napad na zunanjega ponudnika storitev IT, ki zagotavlja ključne storitve za sistemsko pomembne finančne institucije, lahko ravno tako negativno vpliva na finančno stabilnost. Podobne učinke si je mogoče predstavljati v zvezi s programskimi izdelki, ki se uporabljajo kot skupne rešitve za celotni finančni sistem, te pa lahko postanejo problematične v primeru nepravilnega delovanja programske opreme zaradi kibernetskega napada. Zato je odpornost[2] kibernetskega omrežja ključna za stabilnost finančnega sistema (Banka Slovenije, 2024).

Kibernetsko kartiranje lahko temelji na dveh različnih pristopih oziroma metodologijah, in sicer:

- Funkcionalni pristop temelji na ideji, da so nekatere funkcije za finančni sistem in finančno stabilnost ključnega pomena. Pri funkcionalnem pristopu so ključne kritične funkcije opredeljene in razdeljene glede na namen zemljevida, nato pa so opredeljene institucije, ki zagotavljajo te funkcije, in sistemi, na katere se te institucije pri zagotavljanju funkcij zanašajo. Na podlagi tega zemljevida lahko identificiramo in spremljamo tveganja koncentracije in kanalov okužbe v finančnem sistemu.

- Institucionalni pristop temelji na ideji, da lahko strukturo finančnega sektorja, finančne povezave in procese povežemo s kibernetskim omrežjem. Kibernetsko omrežje po tem pristopu se obravnava kot virtualno plast finančnega omrežja, ki jo sestavljajo vse komponente IKT, ki jih finančne institucije uporabljajo za svoje poslovanje. Institucije za ponujanje svojih finančnih storitev uporabljajo programsko opremo, strojno opremo ter druge komponente IKT, ki jih zagotavljajo ponudniki IKT storitev (tretjih oseb). S kartiranjem finančnega omrežja (tj. finančnega sistema) na kibernetsko omrežje lahko identificiramo povezave med ključnimi ponudniki IKT tretjih oseb, ki jih uporabljajo sistemsko pomembne finančne institucije. Ta pristop omogoča razkritje skupnih ponudnikov IKT (npr. ponudnikov storitev v oblaku) v finančnem sektorju. Tudi s tem orodjem lahko nadzorniki finančnega sektorja identificiramo tveganje koncentracije[3] v omrežju in prenosne kanale kibernetskega tveganja na finančni sistem.

Banke Slovenije je razvila kibernetsko kartiranje, ki temelji na institucionalnem pristopu. Za ta pristop smo se odločili, ker sta naš bančni sistem in tehnološki trg v primerjavi z ostalimi večjimi državami EU manj obsežna, orodje, temelječe na tem pristopu pa ni preveč kompleksno z vidika vzdrževanja. Kibernetsko kartiranje omogoča naslednje oblike dodane vrednosti za nadzorniško spremljanje kibernetskega tveganja:

- identifikacija ključnih točk finančnega in kibernetskega sistema,
- pregled nad interakcijami med finančnim in kibernetskim omrežjem,
- zaščita kritične infrastrukture na nacionalni ravni in
- upravljanje sistemskih kibernetskih tveganj.

[2] Kibernetsko odpornost lahko opredelimo kot sposobnost banke ali druge finančne institucije, da uresničuje svoje poslanstvo s predvidevanjem in obvladovanjem kibernetskih tveganj ter hitrim okrevanjem po kibernetskih incidentih.

[3] Tveganje koncentracije izhaja iz velike izpostavljenosti bank do nekaterih IKT ponudnikov storitev. To tveganje bi se lahko realiziralo v primeru, ko bi zaradi nedostopnosti ključnega IKT ponudnika banke ne bi mogle normalno poslovati oziroma izvajati ključnih ekonomskih funkcij.

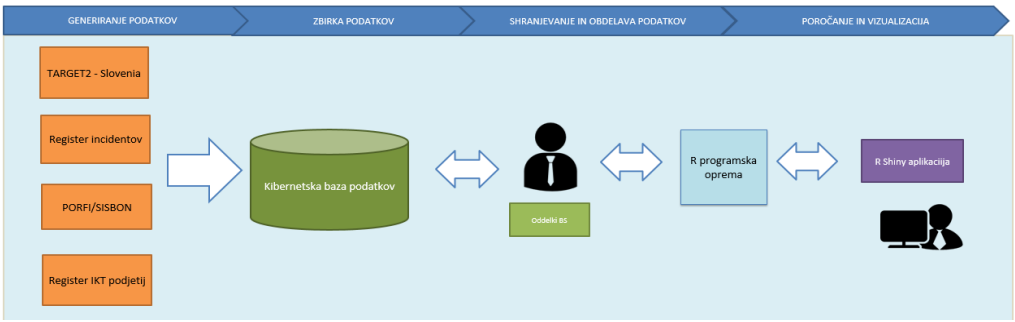
3 Kibernetska zbirka podatkov in metodologija kibernetskega kartiranja

Pred razvojem orodja za kibernetsko kartiranje je potrebno vzpostaviti kibernetsko bazo podatkov in določiti metodologijo, na podlagi katere se ustvari finančno in kibernetsko omrežje. Kibernetska zbirka podatkov ne zajema samo podatkov o IKT ponudnikih ter poročil o kibernetskih incidentih, ampak tudi finančne podatke posameznega subjekta nadzora. Taka zbirka podatkov je podlaga za razvoj in delovanje orodja za kibernetsko kartiranje, ki temelji na institucionalnem pristopu.

3.1 Kibernetska zbirka podatkov

Za razvoj orodja kibernetskega kartiranja potrebujemo podatke: o domačih plačilih in poravnavah (nahajajo se v sistemu TARGET2), in finančne podatke o poslovanju bank (poročanje finančnih institucij in SISBON). V kibernetski zbirki podatkov se nahajajo podatki o bilančni vsoti, tržnem deležu bank, dobičku, medsebojne terjatve med bankami, kapitalu in komitentih bank. Za potrebe vzpostavitve kibernetske mreže sta vzpostavljena tudi dva registra. Prvi register zajema poročila o kibernetskih incidentih, ki jih bančni zavezanci poročajo centralni banki. V teh poročilih se nahajajo ključni podatki in informacije o vplivu incidenta na poslovanje bank. Drugi register zajema seznam vseh ponudnikov IKT storitev, ki nudijo storitve bankam.

Slika 2: **Arhitekturna zasnova sistema**



Vir: Banka Slovenije

Na sliki 2 je prikazan podatkovni tok prenosa finančnih in kibernetskih podatkov v kibernetsko bazo podatkov. Do podatkov je možno dostopati bodisi na direktni način z dostopom do baze podatkov ali pa preko vnaprej pripravljenih nadzorniških in statističnih poročil, ki so namenjena spremljanju kibernetske varnosti bančnega sektorja. Nadzorniška in statistična poročila zajemajo ključne operativne in finančne indikatorje, ki nam signalizirajo sistemsko kibernetsko tveganje na nivoju bančnega sistema. Kibernetska baza podatkov je tudi podlaga za razvoj orodja in aplikacije za kibernetsko kartiranje.[4]

Rezultate orodja za kibernetsko kartiranje je možno deliti z večjim številom nadzornikov, ki so odgovorni za spremljanje operativnega oziroma kibernetskega tveganja, bodisi na mikrobonitetnim ali pa makrobonitetnem nivoju (Borghard, 2018).

[4] Orodje za kibernetsko kartiranje je razvito s pomočjo R programske opreme, medtem ko je vizualizacija orodja razvita s pomočjo R Shiny.

3.2 Metodologija kibernetskega kartiranja

Kibernetsko kartiranje se začne z zbirnim pogledom na finančni sektor iz ptičje perspektive. Opredelitev sistemsko pomembnih institucij v finančnem omrežju je predpogoj za analizo morebitnih destabilizacijskih vplivov kibernetskega omrežja na finančno omrežje. Uspešen kibernetski napad, ki prizadene le enega od teh sistemsko pomembnih akterjev, se namreč lahko razvije v neposredno grožnjo za finančni sistem kot celoto (Bank of England, 2022a).

Kibernetski napad na kritično število nesistemsko pomembnih subjektov lahko prav tako predstavlja tveganje za operativno in finančno stabilnost (ESRB, 2020b). Ni nujno, da je ta kritična masa sestavljena zgolj iz subjektov enega sektorja. Hekerske skupine bi namreč lahko izvedle kibernetski napad na skupino heterogenih institucij, ki pripadajo različnim sektorjem, vendar vse uporabljajo isto programsko opremo ali istega ponudnika storitev IKT v oblaku. Čeprav je torej finančni sistem mogoče razdeliti na posamezne sektorje, je potrebno kibernetska tveganja vedno obravnavati tudi z medsektorskega vidika (Bank of England, 2021). V finančno in kibernetsko mrežo torej morajo biti vključene institucije, ki so pomembne za delovanje bančnega sistema ter lahko v primeru motenj, ki jih lahko povzročijo kibernetski napadi ogrožajo finančno stabilnost (glej tabelo 1).

Tabela 1: **Institucije, ki so pomembne za delovanje bančnega sistema**

Sektor	Sistemski pomen
Banke	Banke razdelimo glede na pomembnost v bančnem sistemu, in sicer jih delimo na: sistemsko pomembne banke, manj pomembne banke in hranilnice ter podružnice. V primeru, da pride do uspešnega kibernetskega napada na sistemsko pomembno institucijo, lahko to vpliva tudi na poslovanje ostalih bank v sistemu.
Finančna infrastruktura	Finančna infrastruktura ima ključno vlogo za delovanje bančnega sistema, saj omogoča obračun in poravnavo plačil (TARGET2), vrednostnih papirjev, izvedenih finančnih instrumentov (KDD) in drugih finančnih transakcij (Bankart).
Nacionalna centralna banka	Centralna banka je najbolj pomembna finančna institucija v omrežju; njeno nedelovanje bi vplivalo na (ne)delovanje finančnega sistema.
Ponudniki IKT storitev	Ključni IKT ponudniki so tisti, ki ponujajo storitve pomembnim finančnim institucijam. V primeru nedelovanja skupnih ponudnikov IKT storitev lahko to ogroža bančno poslovanje.
Ponudniki oblačnih storitev	Vse več bank najema storitve pri oblačnih ponudnikih. To povečuje izpostavljenost in tveganja za banke, če oblačne storitve niso dostopne zaradi kibernetskih napadov. Še večji problem se pojavi, če je več bank odvisnih od istega oblačnega ponudnika.
Drugi sektorji	Subjekti, ki ponujajo storitve sistemsko pomembnim finančnim institucijam ter bi v primeru motenj lahko to vplivalo na njihovo poslovanje (medsektorski vpliv).

Vir: Banka Slovenije

Vsak kibernetski napad na sistemsko pomembno institucijo v finančnem omrežju nima sistemskega vpliva, vendar kljub temu predstavlja potencialno kibernetsko grožnjo za finančno stabilnost (IMF, 2024). To je predvsem odvisno od tega, na katere ključne ekonomske funkcije bo kibernetski napad vplival ter koliko časa bo trajala prekinitev poslovanja (Bank of England, 2022b). Orodje za kibernetsko kartiranje prikaže, kje v finančnem sistemu so se pojavili kibernetski incidenti ter kako so posredno ali pa neposredno vplivali na ostale sistemsko pomembne institucije v finančnem in tehnološkem omrežju.

Z orodjem za kibernetsko kartiranje spremljamo in identificiramo:

- V katerih finančnih institucijah se je zgodil kibernetski incident ter čas reševanja, ki je bil potreben za reševanje dogodka in potencialni vpliv na poslovanje ostalih finančnih institucij (kanali okužbe). Na podlagi tega lahko identificiramo ali je finančna institucija, ki je bila deležna kibernetskega napada, sposobna zagotoviti neprekinjeno poslovanje. Načrt obravnava dogodke, ki predstavljajo veliko tveganje za prekinitev poslovanja in običajno vključuje sekundarno oziroma rezervno lokacijo.

- Sistemsko pomembne motnje zaradi kibernetskega dogodka (vsaka prekinitev poslovanja sistemsko pomembnih institucij oziroma njihovih ključnih ekonomskih funkcij, ki ne bi bile razrešene do konca delovnega dne). Identifikacija takih preteklih dogodkov omogoča hitrejše ukrepanje v primeru dejanskega incidenta, kar lahko prepreči razvoj sistemskega dogodka, ki bi lahko ogrozil poslovanje finančnih institucij.

- Kanale prenosa kibernetskega šoka na celoten finančni sistem ter potencialne finančne izgube zaradi kibernetskega dogodka. Spremljamo lahko posredne in neposredne finančne izgube, ki jih povzročijo kibernetski napadi.

- Kibernetski dogodki, ki vplivajo na delovanje ključnih ekonomskih funkcij finančnega sistema lahko spodkopavajo zaupanje v finančne institucije, kar pa je težko meriti in oceniti. Ocena vpliva kibernetskega dogodka na zaupanje javnosti v finančni sistem je posledično predvsem kvalitativna. Vpliv na zaupanje v finančni sistem lahko merimo z naslednjimi indikatorji: medijska pokritost dogodka, trajanje in obseg medijske pokritosti (na primer medregionalni ali meddržavni). Ti dejavniki lahko ustvarijo vtis o morebitnem destabilizacijskem vplivu kibernetskega dogodka prek kanala zaupanja.

Tabela 2: **Subjekti na zemljevidu**

Terminologija	Opis
Subjekti finančnih storitev	Centralne banke, banke, zavarovalnice, investicijski skladi, borznoposredniške hiše
Subjekti finančne infrastrukture	Upravljavci plačilnih sistemov, borze, deponenti, ponudniki informacijskih storitev
Finančni sektor	Vse od naštetega (subjekti finančnih storitev in infrastrukture)
Subjekti IKT	Prodajalci strojne in programske opreme, ponudniki storitev v oblaku, ponudniku telekomunikacijskih storitev, ponudniki storitev IT
Komponente IKT	Strojna in programska oprema, omrežja, podatkovni centri

Vir: Banka Slovenije

Prvi korak pri razvoju orodja je definiranje vozlišč. Vozlišča običajno predstavljajo centralne banke, poslovne banke, zavarovalnice, investicijska podjetja in ponudniki storitev IKT. Pri definiranju ključnih vozlišč je pomembna tudi definicija zemljevidnih slojev, ki jih sestavljajo: podatkovni tok, organizacijska in tehnološka odvisnost, ki skupaj tvorijo mrežo povezav ter vozlišč med finančnim in tehnološkim sektorjem (glej tabelo 2). Podatkovni tok med finančnimi institucijami predstavljajo bodisi transakcije ali obveznosti med bankami, medtem ko pri ponudnikih storitev IKT povezave predstavljajo delež vseh storitev ponudnikov IKT storitev, ki jih posamezni IKT ponudnik nudi posamezni banki na trgu. Vozlišča se še dodatno ovrednoti po pomembnosti v sistemu s kazalniki kot so tržni delež, število komitentov in bilančna vsota. Mreže povezav med finančnim

in tehnološkim sektorjem ustrezno utežimo na podlagi tržnega deleža, saj s tem dobimo bolj realno sliko tveganja v bančnem sektorju. Kibernetsko kartiranje vključuje tudi podatke o kritičnih kibernetskih incidentih, ki so se zgodili v bančnem sistemu ter njihov potencialni vpliv na poslovanje ostalih subjektov v mreži.

Tabela 3: **Terminologija kibernetskega kartiranja (določitev vozlišč)**

Nivo	Prikaz subjektov	Opomba
Finančne povezave	Subjekti finančnega nadzora	Osredotočenost na tehnične povezave
	Finančna infrastruktura	
Organizacijska odvisnost	Subjekti finančnih storitev	V finančnem sektorju
	Finančna infrastruktura	Finančni sektor – IKT
	Subjekti IKT	IKT - IKT
Tehnološka odvisnost	Subjekti finančnih storitev	Vpliv organizacijske odvisnosti
	Finančna infrastruktura	
	Subjekti IKT	
	Strojna oprema	
	Programska oprema	
	Omrežje	

Vir: Banka Slovenije

Kibernetsko omrežje zajema vse tiste elemente IKT, ki tvorijo osnovno infrastrukturo za vse operativne procese, ki potekajo v finančnem omrežju. Ključni tehnični elementi infrastrukture IKT so programska in strojna oprema ter vgrajene naprave, ki se uporabljajo za delovanje aplikativne programske opreme (Brauchle in ostali, 2020). Zagotavljanje takih storitev banke vse bolj pogosto oddajo v zunanje izvajanje tretjim ponudnikom IKT storitev (glej tabelo 3).

Ključne komponente kibernetskega omrežja in tveganja v povezavi z kibernetskimi napadi so sledeča:

- Programska oprema - velika večina kibernetskih napadov se zgodi s pomočjo zlonamerne programske opreme, katero hekerji običajno uporabijo za vdor v informacijski sistem in ga namerno poškodujejo.

- Strojna oprema - Strojno opremo je mogoče spreminjati, na primer z dodatnimi strukturnimi komponentami, spreminjanjem obstoječih vezij, poseganjem v čipe ali spreminjanjem vdelane programske opreme. Primeri hekerskih vdorov so posegi v delovanje bankomatov, terminalov za plačila in kreditnih kartic. Skupni računalniški centri, ki jih uporablja več bank, lahko krepijo tveganje koncentracije.

- Računalništvo v oblaku - večina ponudnikov storitev v oblaku ponuja podobne storitve številnim finančnim institucijam. Če je večje število finančnih institucij odvisnih od enega oblačnega ponudnika, lahko nastane tveganje koncentracije. Uspešen kibernetski napad na oblačnega ponudnika lahko povzroči slabšo razpoložljivost storitve in ogrozi zaupnost ali celovitost podatkov.

- Zunanje izvajanje IKT storitev - vse več finančnih institucij prenaša svoje storitve v izvajanje zunanjim ponudnikom IKT, kar povečuje njihovo izpostavljenost, če pride do resnega kibernetskega napada na izvajanje ključne ekonomske

funkcije, katere delovanje podpirajo tudi zunanji ponudniki IKT. Večji kibernetski napadi lahko vplivajo na to, da računalniški centri ali bankomati določen čas ne delujejo (IOSCO, 2020).

Vse te ključne komponente IKT so zajete in prikazane v kibernetskem omrežju ter so posredno ali neposredno povezane s finančnimi institucijami, ki skupaj tvorijo kibernetsko omrežje. V primeru, da pride do kibernetskega napada na eno izmed ključnih komponent IKT, lahko to povzroči nedelovanje storitev, ki so pomembne za banke in njene komitente. Zato je ključno, da imajo banke in hranilnice vzpostavljene načrte nepreki-njenega poslovanja (Nish in Naumaan, 2019).

3.3 Vzpostavitev bančnega in kibernetskega omrežja

Vzpostavitev bančnega in kibernetskega omrežja poteka postopoma, kar pomeni, da pričnemo v prvem koraku z vzpostavitvijo bančnega omrežja. Bančno omrežje sestavljajo banke in hranilnice, ki na trgu poslujejo z gospodarstvom. Banke klasificiramo glede na pomembnost v bančnem sistem, in sicer: (i) sistemsko pomembne banke, (ii) manj pomembne banke (brez hranilnic) in (iii) hranilnice ter podružnice. V naslednjem koraku potem dodatno opredelimo pomembnost posamezne banke v bančnem sistemu. Vsak subjekt na trgu je opredeljen kot vozlišče, ki je ovrednoteno po pomembnosti v sistemu s kazalniki kot so tržni delež, število komitentov in bilančna vsota. Pomembnost kazalnika določa velikost vozlišča v sistemu, višja kot je vrednost kazalnika, bolj je subjekt pomemben za bančni sistem. Z ovrednotenjem vozlišč dobimo ključne subjekte, ki jih je treba v naslednjem koraku medsebojno povezati v bančno omrežje. Bančno omrežje tvorijo finančne povezave, ki temeljijo na poravnavi medsebojnih domačih plačil in obveznosti med bankami. S finančnimi povezavami dobimo pregled nad finančnem poslovanjem bank, možnostmi okužbe in koncentracijo tveganja, kadar pride do resnega kibernetskega napada.

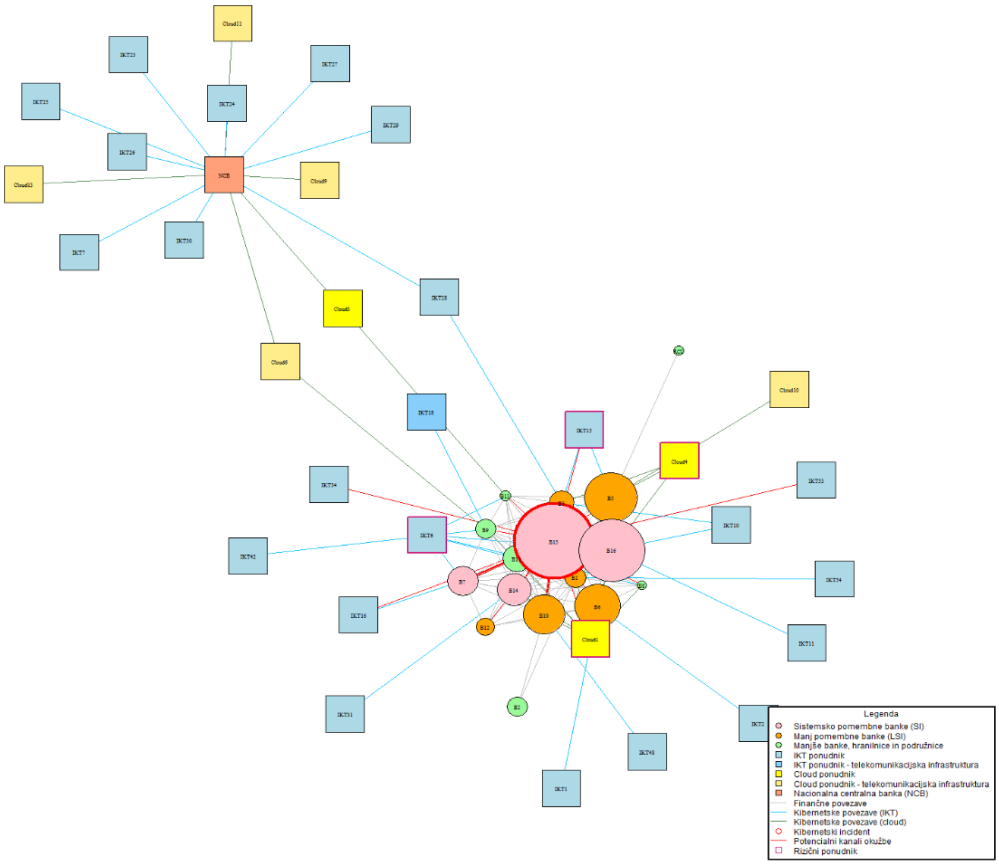
Ko je bančno omrežje vzpostavljeno, sledi oblikovanje kibernetskega omrežja, ki temelji na povezavah med različnimi tehnološkimi subjekti na trgu. Gre za različne zunanje ponudnike storitev IKT (vključno z oblačnimi in telekomunikacijskimi). V kibernetskem omrežju so prikazani samo ključni tehnološki subjekti, ki ponujajo storitve IKT bančnemu sektorju. Povezave med tehnološkimi subjekti na trgu so določene na podlagi poslovnega sodelovanja. To pomeni, da določena podjetja IKT najemajo storitve, kot so na primer strojna, programska oprema ali pa najem oblačne storitve, pri ostalih podjetjih IKT.

Ključne povezave med tehnološkimi subjekti tvorijo kibernetsko omrežje, ki je izredno prepleteno in medsebojno odvisno. To pomeni, da lahko uspešni kibernetski napad prizadene določena tehnološka podjetja, ki nudijo določene tehnološke storitve bankam, kar lahko povzroči nedelovanje določenih podpornih bančnih informacijskih sistemov. Zato je pomembno, da imamo na zemljevidu prikazane povezave med bančnim in tehnološkim omrežjem. Te povezave moramo ustrezno utežiti, npr. s tržnim deležem[5], kar omogoči bolj realno sliko vpliva kibernetskega incidenta na delovanje bančnega in tehnološkega sektorja. Ob uporabi te uteži se prikažejo najbolj pomembni tehnološki subjekti v omrežju, kar nadzornikom bančnega sektorja omogoči, da se lahko osredotočijo na ključne ranljivosti v sistemu.

[5] Podatkovni tok med finančnimi institucijami predstavljajo transakcije ali obveznosti med bankami, pri ponudnikih storitev IKT pa delež storitev posameznega ponudnika v vseh storitvah zunanjih ponudnikov IKT storitev za posamezno banko na trgu. Vozlišča se s kazalniki, kot so tržni delež, število komitentov in bilančna vsota, še dodatno ovrednotijo po pomembnosti v sistemu.

Kibernetsko omrežje vključuje tudi podatke o kibernetskih incidentih, ki so se pojavili in zgodili tako v bančnem kot tudi tehnološkem sektorju ter njihov potencialni vpliv na poslovanje drugih subjektov v kibernetskem omrežju. Informacije o preteklih resnih kibernetskih incidentih so pomembne tudi za napovedovanje, kje lahko v prihodnje pričakujemo incidente v bančnem in tehnološkem omrežju. Tako na bančnem kot tudi na kibernetskem omrežju incidente obarvamo z rdečo barvo. Z vzpostavitvijo bančnega in kibernetskega omrežja ter medsebojnih povezav (medbančne, med tehnološke in bančno-tehnološke) se pokaže celovit pregled tretjih (zunanjih) ponudnikov storitev IKT, ki jih pri svojem poslovanju uporabljajo banke. S pomočjo kibernetskega omrežja vidimo, da imamo na trgu tretje (zunanje) ponudnike storitev IKT, ki več bankam ponujajo podobne storitve. Z vzpostavitvijo bančnega in kibernetskega omrežja lahko nadzorniki lažje spremljajo koncentracijo tveganja v sistemu kot tudi kanale prenosa kibernetskega tveganja v bančni sistem (glej sliko 3).

Slika 3: **Bančno in kibernetsko omrežje**



Vir: Banka Slovenije

Ker je nacionalna centralna banka ključna institucija v finančnem sistemu, je pomembno, da je vključena v bančno in kibernetsko omrežje. Pri oblikovanju omrežja je pomembno spremljati finančne ter tehnološke povezave nacionalne centralne banke s poslovnimi bankami, plačilnimi ponudniki in tretjimi (zunanjimi) ponudniki storitev IKT.

3.4 Napovedi kibernetskega omrežja s pomočjo različnih tehnik strojnega učenja

Orodje za kibernetsko kartiranje obsega tudi napoved omrežja za prihodnje leto. Pri napovedovanju bodočega kibernetskega omrežja so bile uporabljene različne tehnike

strojnega učenja. Tehnike temeljijo na napovedovanju časovnih vrst, ki so namenjene oceni prihodnjih vrednosti na podlagi predhodno ugotovljenih vrednosti. Prva uporabljena tehnika za napovedovanje kibernetskega zemljevida je bila TBATS, ki je zasnovana za napovedovanje časovnih vrst z več sezonskimi obdobji. TBATS je metoda napovedovanja modeliranje podatkov časovnih vrst, katere glavni cilj je napovedovanje časovnih vrst s kompleksnimi sezonskimi vzorci z uporabo eksponentnega glajenja (glej tabelo 4). Napoved (za eno leto vnaprej) prikaže bodoče povezave med subjekti finančnega sektorja, ponudniki tehnologij in tehnološkimi rešitvami ter potencialna tveganja v bančnem sistemu (vključno z Banko Slovenije), s čimer pokaže bodoča sistemsko pomembna vozlišča, kjer je prisotno tveganje koncentracije in možnosti okužbe v bančnem sistemu.

Tehnika TBATS uporablja različne metode eksponentnega glajenja in jo je mogoče opisati z naslednjimi enačbami:

Tabela 4: **Opis tehnike TBATS**

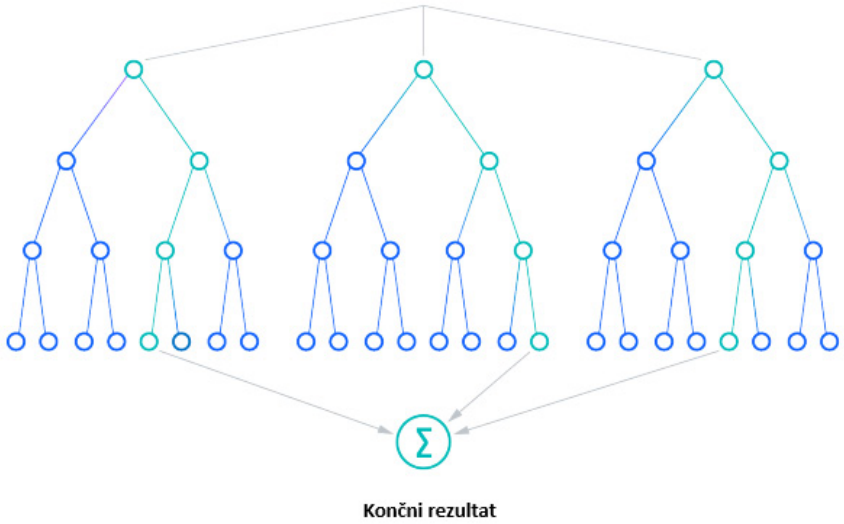
Model	**Opis modela**
$y_t^{(\lambda)} = l_{t-1} + \Phi b_{t-1} + \sum_{i=1}^{T} s^{(i)}_{t-mi} + d_t$	$y_t^{(\lambda)}$ = časovna vrsta v trenutku t $s_t^{(i)}$ = i-ta sezonska komponenta
$l_t = l_{t-1} + \Phi b_{t-1} + \alpha d_t$	l_t = lokalni nivo
$b_t = \Phi b_{t-1} + \beta d_t$	b_t = trend z blaženjem
$d_t = \sum_{i=1}^{p} \varphi_i d_{t-1} + \sum_{i=1}^{q} \Theta_i e_{t-1} + e_t$	d_t = ARMA(p, q) in ostanki e_t = šum po Guassanovi metodi
Sezonski del	**Parametri modela**
$s_t^{(i)} = \sum_{j=1}^{(k_i)} s^{(i)}_{j,t}$	T - Obseg sezonskosti m_i - dolžina i-tega sezonskega obdobja
$s^{(i)}_{j,t} = s^{(i)}_{j,t-1} \cos(\omega i) + s^{*(i)}_{j,t-1} \sin(\omega_i) + \aleph_1^{(i)} d_t$ $s^{*(i)}_{j,t} = -s^{(i)}_{j,t-1} \sin(\omega i) + s^{*(i)}_{j,t-1} \cos(\omega_i) + \aleph_2^{(i)} d_t$	λ - Box-Cox transformacija α, β – glajenje Φ - blaženje trenda
$\omega_i = 2\,л\,j\,l\,m_i$	φ_i, Φ_i - ARMA[6] (p, q) koeficienti $\aleph_1^{(i)}$, $\aleph_2^{(i)}$ – sezonsko glajenje (dve za vsako obdobje)

Vir: (De Livera in drugi, 2011)

Druga tehnika, uporabljena za napovedi, temelji na naključno odločitvenem gozdu (angl. random forest). Pri njej je uporabljen algoritem strojnega učenja, ki rezultate več od-ločitvenih dreves združi v en rezultat, ki je podlaga za napovedovanje bodočega kibernetskega omrežja (Schonlau in ostali, 2020). Algoritem naključnega odločitvenega gozda temelji na treh parametrih, ki jih je treba nastaviti pred učenjem, in sicer: velikost vozlišča (število komitentov, bilančna vsota), število dreves (bank, IKT ponudnikov) in število vzorčenih lastnosti (transakcije, obveznosti, poslovanje med bankami in IKT ponudniki). Nato se lahko klasifikator naključnega odločitvenega gozda uporabi za reševanje problemov regresije ali klasifikacije. Algoritem naključnega odločitvenega gozda je sestavljen iz zbirke odločitvenih dreves, vsako drevo v zbirki pa je sestavljeno iz vzorca podatkov, vzetega iz učne množice z zamenjavo, ki se imenuje zagonski vzorec (glej sliko 4).

[6] Pri statistični analizi časovnih vrst nam modeli kot so ARMA (avtoregresivna drseča sredina) omogočajo enostaven opis stacionarnega stohastičnega procesa s pomočjo dveh polinomov, enega za avtoregresijo in drugega za drseče povprečje.

Slika 4: **Napoved s pomočjo odločitvenih gozdov**



Vir: Banka Slovenije

Končni rezultat predstavlja napoved bodočih povezav med subjekti finančnega sektorja, ponudniki tehnologij in tehnološkimi rešitvami ter potencialna kibernetska tveganja v bančnem sistemu in tehnološkem sektorju. Napoved s pomočjo naključno odločitvenih gozdov temelji na učenju tako iz preteklih dogodkov kot tudi preteklih napovedi, s čimer se skozi čas napovedi bodočega kibernetskega omrežja nenehno izboljšujejo.

Tretja tehnika strojnega učenja, uporabljena za napovedi, temelji na regresiji podpornih vektorjev (angl. support vector regression). Uporablja se za napovedovanje časovnih vrst, zlasti cen delnic, pa tudi kibernetskih napadov in ostalih potencialnih tveganj na področju poslovanja finančnih institucij. Cilj regresije podpornih vektorjev je najti funkcijo, ki napoveduje zvezno ciljno spremenljivko in pri tem poišče razliko med napovedanimi vrednostmi in dejanskimi podatkovnimi točkami. Regresija podpornih vektorjev določi razpon okoli napovedane regresijske premice, njen cilj pa je prilagoditi premico znotraj tega razpona in pri tem čim bolj zmanjšati napako napovedi. Pri regresiji podpornih vektorjev so podatkovne točke, ki so najbližje regresijski premici in določajo razliko, znane kot podporni vektorji. Te točke imajo ključno vlogo pri določanju regresijskega modela. Regresija podpornih vektorjev poskuša najti regresijski model z razponom okoli napovedanih vrednosti, ki omogoča ravnovesje med prilagajanjem podatkom in izogibanjem pretiranemu prilagajanju. Posebej uporabna je pri obravnavi nelinearnih razmerij, z izbiro funkcij jedra pa jo je mogoče prilagoditi različnim problemskim področjem, tudi napovedovanju bodočega kibernetskega omrežja ter potencialnih tveganj za bančni sektor zaradi resnih kibernetskih incidentov.

Napovedi bodočega kibernetskega zemljevida posameznih tehnik strojnega učenja smo tudi testirali na preteklih podatkih. Tehnike strojnega učenja podajo ocene bilančne vsote, števila komitentov (fizičnih in pravnih oseb), tržnega deleža, pojavnosti kibernetskih incidentov in plačilnega prometa za naslednje leto. Odstopanja napovedi od dejanskih vrednosti na nivoju bančnega sistema znašajo med 6 % in 10 %. Razlike med odstopanji po posameznih omenjenih tehnikah so različne, zato je pri napovedih smiselno uporabiti tudi kombinacijo vseh treh tehnik strojnega učenja, kar izboljša verjetnost napovedi.

Napovedi kibernetskih incidentov in bodočih IKT ponudnikov so zelo natančne, saj algoritmi na podlagi preteklih dogodkov predvidevajo, kje v bančnem sistemu se bodo pojavili incidenti in povezave med bankami ter IKT ponudniki. Napovedi z različnimi tehnikami strojnega učenja napovedujejo naslednje finančne podatke: bilančno vsoto, število fizičnih in pravnih oseb, ki imajo odprte račune pri bankah, tržni delež bank ter število kritičnih kibernetskih incidentov, ki so jih poslovne banke poročale centralni banki. V napoved so vključeni podatki o domačih plačilih in informacije o IKT ponudnikih. Na podlagi rezultatov opisanih tehnik strojnega učenja je bilo ocenjeno odstopanje napovedi od dejanskih vrednosti, ki smo jih klasificirali v štiri razrede (glej tabelo 5).

Tabela 5: **Primerjava napovedi s pomočjo različnih tehnik strojnega učenja**

Banka	Bilančna vsota			Število fizičnih oseb			Število pravnih oseb			Tržni delež			Kibernetski incidenti		
	TBATS	RF	SVR	TBATS	RF	SVR	TBATS	RF	SVR	TBATS	RF	SVR	TBATS	RF	SVR
B1	1%	6%	5%	1%	1%	9%	4%	17%	20%	8%	6%	6%	0%	0%	0%
B2	1%	1%	2%	1%	1%	5%	10%	25%	17%	6%	8%	4%	0%	0%	0%
B3	4%	4%	5%	0%	0%	1%	15%	15%	15%	7%	5%	6%	0%	0%	6%
B4	1%	4%	3%	10%	10%	19%	1%	7%	6%	10%	1%	5%	0%	0%	0%
B5	12%	2%	3%	1%	1%	2%	2%	56%	86%	1%	1%	4%	0%	0%	0%
B6	4%	5%	8%	3%	3%	1%	5%	5%	6%	5%	7%	8%	0%	0%	0%
B7	6%	5%	5%	1%	1%	2%	3%	22%	15%	8%	5%	5%	0%	1%	6%
B8	15%	11%	19%	11%	11%	3%	4%	14%	17%	5%	13%	21%	0%	0%	0%
B9	10%	14%	18%	1%	1%	0%	10%	5%	5%	11%	16%	18%	0%	0%	0%
B10	1%	7%	7%	2%	2%	4%	3%	7%	7%	14%	8%	9%	0%	0%	0%
B11	7%	8%	9%	1%	1%	0%	1%	4%	5%	13%	6%	6%	0%	0%	0%
B12	4%	3%	0%	15%	15%	14%	4%	8%	10%	2%	1%	1%	0%	0%	0%
B13	4%	3%	7%	3%	3%	7%	4%	11%	9%	5%	1%	4%	0%	0%	0%
B14	4%	9%	12%	0%	0%	1%	3%	14%	32%	1%	9%	14%	0%	0%	0%
B15	10%	2%	0%	0%	0%	0%	2%	10%	10%	5%	0%	0%	0%	8%	6%
SISTEM	6%	4%	6%	1%	1%	0%	2%	10%	11%	5%	5%	7%	0%	3%	0%

Barvna lestvica		
	Zelo natančna napoved	Odstopanje od dejanske vrednosti znaša manj kot 5 %.
	Dobra napoved	Odstopanje od dejanske vrednosti znaša med 5 % in 10 %.
	Razumna napoved	Odstopanje od dejanske vrednosti znaša med 11 % in 20 %.
	Netočna napoved	Odstopanje od dejanske vrednosti znaša več kot 20 %.

Vir: Banka Slovenije
Opomba: TBATS je namenjena napovedovanju časovnih vrst z več sezonskimi obdobji. Kratica RS pomeni naključni odločitveni gozdovi (angl. random forest). Kratica SVR pomeni regresija podpornih vektorjev (angl. support vector regression) name-njena napovedovanju časovnih vrst.

Najboljšo napoved bodočega kibernetskega omrežja je podala tehnika TBATS. Odstopanja napovedi od dejanskih vrednosti znašajo na nivoju sistema dobre 4 %, kar pomeni, da ta tehnika poda zelo natančne napovedi. Še boljši rezultati so pri napovedi bodočih kibernetskih incidentov, saj znaša odstopanje od dejanskega števila zgolj 1 %.

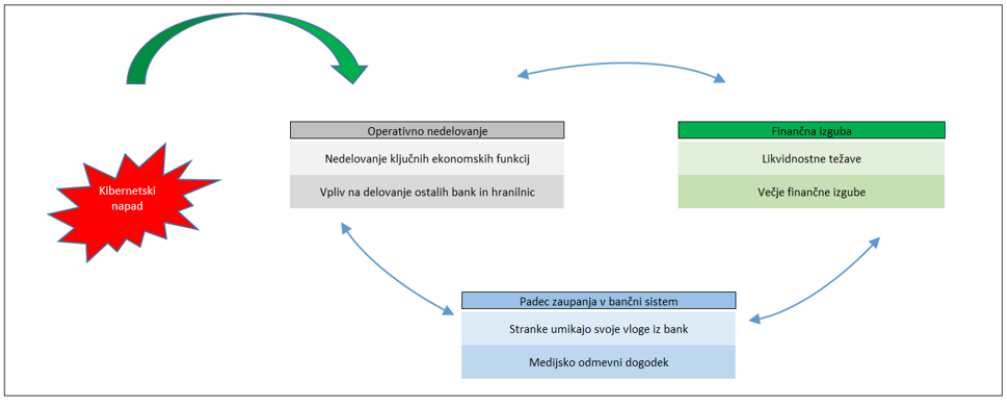
Tehniki, ki temeljita na naključnih odločitvenih gozdovih in regresiji podpornih vektorjev vrneta nekoliko slabše rezultate, in sicer odstopanja napovedi od dejanskih vrednosti znašajo na nivoju sistema med 5 % in 6 %, kar kljub temu predstavlja dobre napovedi.

4 Uporaba orodja za spremljanje sistemskega kibernetskega tveganja

Orodje za kibernetsko kartiranje je namenjeno spremljanju in identificiranju kibernetskih ranljivosti tako na nivoju posameznih bank kot tudi bančnega sistema. Z vidika finančne stabilnosti in makrobonitetne politike nas zanimajo sistemski učinki posameznega kibernetskega napada na bančni sistem (Prenio in Restoy, 2022). Vpliv kibernetskega napada na finančno stabilnost se spremlja s treh vidikov: (i) operativnega (ne)delovanja ključnih ekonomskih funkcij in prenosa tega nedelovanja na ostale banke, (ii) višine finančnih izgub (v povezavi s trajanjem dolgoročnega nedelovanja ključnih ekonomskih funkcij) in (iii) padca zaupanja v bančni sistem. Spremljamo, na kakšen način kibernetski incidenti vplivajo na poslovanje posamezne banke, ostalih bank in zunanjih ponudnikov IKT, ki bankam nudijo storitve (glej sliko 5).

Z orodjem se spremlja neposredno in posredno finančno izgubo ključnih ekonomskih funkcij na nivoju posameznih bank kot tudi bančnega sistema. Če kibernetski napad za dlje časa ohromi delovanje ključnih operacij poslovanja, to pomeni izgubo dostopa do finančnih sredstev in možnosti poravnave obveznosti, zato lahko stranke in tržni udeleženci izgubijo zaupanje v bančni sistem. Če gre za medijsko odmevni dogodek, ta lahko močno vpliva na zaupanje javnosti v bančni sistem, zato je pomembno, da banke izvedejo ustrezne medijske kampanje, ki so namenjene povrnitvi zaupanja javnosti v bančni sistem.

Slika 5: **Vpliv kibernetskega napada na finančno stabilnost in potencialni kanali okužbe v bančnem sistemu**



Vir: Banka Slovenije

Naslednja pomembna informacija, ki jo je mogoče pridobiti s pomočjo orodja, je spremljanje potencialnih kanalov okužbe v bančnem sistemu. Z orodjem spremljamo dva tipa potencialnih okužb, ki se lahko pojavita v bančnem sistemu zaradi kibernetskega napada, in sicer operativno in finančno okužbo[7]. Kibernetski napad v prvi vrsti vpliva na operativno delovanje bank in podjetij IKT, kar lahko povzroči operativno okužbo. To pomeni, da nedelovanje ključnih ekonomskih funkcij pri eni banki vpliva na delovanje ekonomskih funkcij tudi pri ostalih bankah, pa tudi na skupne ponudnike IKT storitev, ki podpirajo delovanje osrednjih bančnih informacijskih sistemov. Težave pri njihovem delovanju pa lahko ponovno vplivajo na poslovanje drugih, neposredno neprizadetih bank.

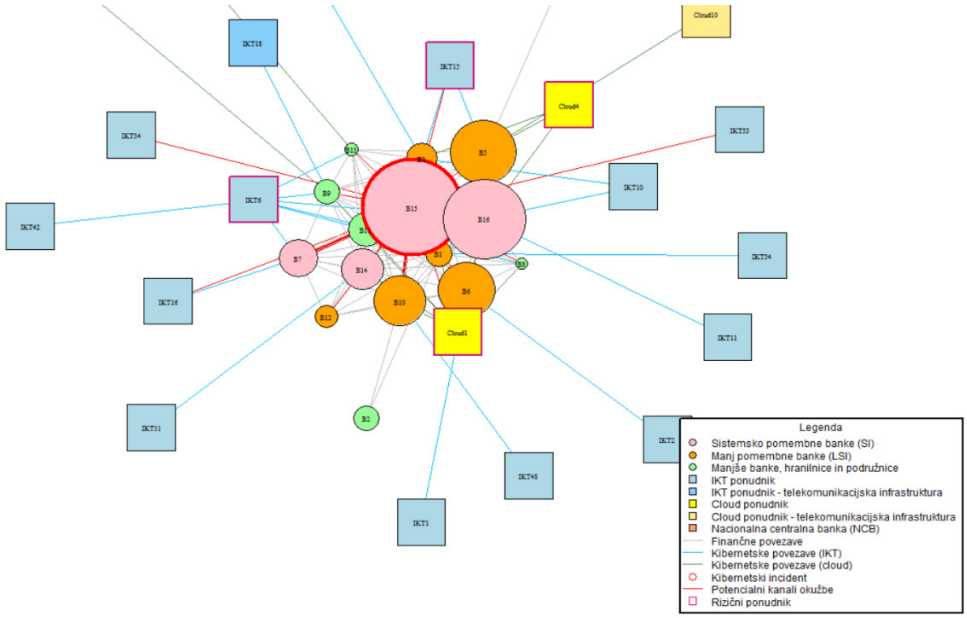
[7] Finančno okužbo bi lahko opredelili, ko stresni dogodek prizadene bančni sektor zaradi medsebojne povezanosti, hitre prodaje sredstev na finančnih trgih ali pa nelikvidnosti. Vir okužbe je torej lahko le posamezen del bančnega sistema, ki lahko na primer zaradi svojih težav vpliva na medbančno poslovanje.

V primeru daljšega nedelovanja bančnih informacijskih sistemov pri večjemu številu bank lahko to vodi v operativno okužbo. Z orodjem se lahko hitro zazna operativno okužbo v omrežju na način, da se spremlja vsak kritični kibernetski incident, ki lahko vpliva na medbančno poslovanje, delovanje ostalih bančnih informacijskih sistemov ali skupnih ponudnikov storitev IKT. Z orodjem se lahko oceni tudi operativno stabilnost bančnega sistema[8], ki ga ogrožajo kritični kibernetski incidenti.

Dlje časa ko ne delujejo ključne ekonomske funkcije in osrednji bančni informacijski sistemi, večji vpliv ima to na finančne izgube in likvidnost bančnega sistema. Poveča se tudi možnost finančne okužbe v sistemu, kar lahko vodi v finančno nestabilnost. Medtem ko neposredne finančne izgube povzroča predvsem izguba provizij zaradi nedelovanja plačilnega prometa in stroški, povezani z vzpostavitvijo predhodnega stanja, so posredne izgube povezane z materializacijo tveganja ugleda.

Posredno finančno izgubo zaradi resnega kibernetskega napada na bančni sistem merimo s številom izgubljenih strank in s tem povezano izgubo prihodkov ter stroški medijskih kampanj, katerih namen je povrnitev ugleda v banke in bančni sistem. Re-sen kibernetski napad lahko ob daljši operativni nestabilnosti vpliva na likvidnost bančnega sistema in tveganje financiranja. Z orodjem se meri in spremlja, kako posamezni kibernetski incidenti vplivajo na odliv vlog na vpogled ter posledično na zmanjšanje čistih prihodkov tako po posameznih bankah kot tudi na nivoju bančnega sistema. S tem identificiramo potencialna tveganja glede poravnave obveznosti (plačilni promet in gotovinsko poslovanje).

Slika 6: **Potencialni kanali okužbe in tveganje financiranja v bančnem sistemi**



Vir: Banka Slovenije

Operativna in finančna okužba lahko vplivata tudi na ostale subjekte na finančnem in tehnološkem trgu. V primeru, da ključni IKT ponudnik ne more poslovati na trgu zaradi kibernetskega napada, lahko to vpliva na poslovanje določenih bank, zavarovalnic in kapitalskega trga. V takih situacijah se srečujemo s potencialnimi kanali okužbe, ki

[8] Operativna stabilnost se nanaša na sposobnost bank, da ohranijo svoje poslovanje brez motenj ključnih ekonomskih funkcij, ki jih lahko povzročijo kibernetski napadi.

jih lahko orodje zazna ter bančnim nadzornikom omogoči lažje ukrepanje in komunikacijo z ostalimi nadzorniki (AZN[9] in ATVP[10]) ter z Uradom za informacijsko varnost RS.

Ugotavljamo, da se na bančnem trgu tveganja koncentrirajo zaradi neposredne izpostavljenosti bank do ključnih ponudnikov storitev IKT in oblačnih ponudnikov storitev. Z orodjem se spremlja in identificira skupne kritične IKT in oblačne ponudnike, ki ponujajo informacijske storitve bankam. To pomeni, da bi v primeru resnega kibernetskega napada na skupnega IKT ali oblačnega ponudnika to lahko vplivalo na zagotavljanje IKT storitev določenim bankam. V primeru, da ključni IKT ponudnik na trgu ne bi mogel zagotavljati informacijskih storitev bankam, bi to vplivalo tudi na poslovanje bančnega sektorja in gospodarstva. Orodje na podlagi algoritma razvrsti ključne IKT ponudnike, ki so pomembni za poslovanje bančnega sektorja.

Zaznati je, da kibernetski incidenti vplivajo tako na neposredno izpostavljenost (poslovni odnosi med različnimi finančnimi institucijami) kot tudi na posredno izpostavljenost (medsebojna povezanost različnih informacijskih sistemov ali skupnih ponudnikov storitev in operativnih sistemov). Uspešen kibernetski napad na ključnega ponudnika IKT storitev lahko vpliva na poslovanje bank. Banke, ki informacijske rešitve in podporo zanje naročajo pri zunanjih izvajalcih in dobaviteljih, so lahko bolj iz-postavljene kibernetskim napadom in incidentom (Aldasoro in ostali, 2020). Pri tehnološki medsebojni povezanosti so problematični predvsem ponudniki tehnoloških storitev (npr. storitve v oblaku), ki lahko ob kibernetskih napadih pospešijo prenos okužbe znotraj bančnega sistema. Na podlagi zaznanih kritičnih kibernetskih incidentov opažamo, da se bančni sistem sooča predvsem s primeri operativne okužbe.

Orodje za kibernetsko kartiranje obsega tudi napoved kibernetskih indikatorjev za naslednje leto. Z orodjem je moč napovedati naslednje ključne operativne in finančne indikatorje s področja kibernetske varnosti bančnega sektorja, kot sledi iz tabele 6.

[9] Agencija za zavarovalni nadzor.
[10] Agencija za trg vrednostnih papirjev.

Tabela 6: **Napoved ključnih kibernetskih indikatorjev**

Indikator	Opis	Opomba
Število prijavljenih kritičnih kibernetskih incidentov	Število prijavljenih kritičnih kibernetskih incidentov centralni banki	Poslovne banke so dolžne poročati kibernetski incident centralni banki na podlagi EBA smernic, ki opredeljujejo kriterije poročanja.
Ocena posredne finančne škode (v tisoč evrih)	Denarni znesek (EUR), ki ga je incident posredno povzročil (npr. stroški povračila škode/odškodnine strankam, morebitni sodni stroški).	Enostransko tveganje. Višja vrednost indikatorja pomeni potencialno večje strukturno sistemsko tveganje.
Ocena neposredne finančne škode (v tisoč evrih)	Denarni znesek (EUR), ki ga je incident neposredno povzročil, vključno s tistimi, ki so potrebni za odpravo incidenta (npr. razlaščena sredstva ali sredstva, stroški zamenjave strojne in programske opreme, dajatve zaradi neizpolnjevanja pogodbenih obveznosti).	
Delež priglašenih kibernetskih incidentov v bančništvu glede na vse incidente v RS	Indikator nam daje informacijo koliko je bančni sektor izpostavljen do kibernetskih incidentov napram ostalim sektorjem.	
Delež kritičnih incidentov glede na vse priglašene incidente	Indikator nam daje informacijo o tem koliko kibernetskih incidentov je kritičnih glede vse priglašene incidente.	
Število Phishing in DDoS napadov	Najbolj pogosti tipi kibernetskih napadov na poslovne banke so bodisi phishing ali DDoS, zato jih na podlagi preteklih trendov napovedujemo.	
Delež proračuna za IT varnost	Indikator nam meri kolik bodo banke namenile svojega proračuna za IT varnost glede na vsa sredstva namenjana IT-ju (razvoj, zunanji izvajalci, infrastruktura itd.).	
Število naprav z zastarelo programsko opremo	Zastarela programska oprema povečuje informacijsko ranljivost posameznih bank in bančnega sistema.	

Vir: Banka Slovenije

Na podlagi prejetih napovedi po posameznih indikatorjih lahko na nivoju bančnega sistema spremljamo tveganja s področja kibernetske varnosti. Z orodjem lahko na-povemo tudi potencialne zlonamerne aktivnosti tako notranjih kot zunanjih akterjev. Te napovedi lahko olajšajo sprejemanje ukrepov, usmerjenih v krepitev kibernetske odpornosti bančnega sektorja.

5 Zaključek in nadaljni koraki

V času pospešene digitalizacije in globalizacije finančnega sektorja je pomembno nadzorniško spremljanje in identificiranje potencialnih kibernetskih groženj (Adelmann in ostali, 2019). Eno izmed takih orodij, ki to omogoča, je kibernetsko kartiranje, ki je namenjeno nadzornikom finančnega sektorja, da lažje spremljajo kibernetsko tveganje ter na podlagi tega tudi ukrepajo, ko zaznajo grožnje, ki bi lahko ogrozile operativno in finančno stabilnost bančnega sistema. Orodje za kibernetsko kartiranje se lahko opredeli kot orodje za upravljanje informacij, ki so ključne za obvladovanje prihodnjih kibernetskih kriz s strani nadzornikov finančnega sektorja (ESRB, 2023). Orodje je ključno za zbiranje, obdelavo in ponovno distribucijo informacij o večjih kibernetskih dogodkih (ESRB, 2024). Namenjeno je tudi obveščanju posameznim bank in ostalih nadzornikov (tako na sektorski kot tudi medsektorski ravni) o večjih kibernetskih dogodkih(glej sliko 6).

Z orodjem in dodatno vizualizacijo je možno hitro razbrati ključne finančne povezave med posameznimi finančnimi subjekti in sektorjem IKT, ki predstavlja kibernetsko omrežje. Kibernetsko omrežje pokriva vse tiste elemente informacijske in komunikacijske tehnologije, ki predstavljajo osnovno infrastrukturo za vse operativne procese v finančnem omrežju. Na podlagi tega smo razvili orodje za kibernetsko kartiranje, ki temelji na institucionalnem pristopu. Značilnost tega pristopa je, da lahko strukturo finančnega sektorja, finančne povezave in procese povežemo s kibernetskim omrežjem. Za ta pristop smo se odločili, ker je tako bančni sistem kot tudi tehnološki trg manj obsežen v primerjavi z ostalimi večjimi državami EU in ni preveč kompleksen z vidika vzdrževanja. Kibernetsko kartiranje za nadzornike finančnega sektorja prinaša dodano vrednost na način, ki omogoča identifikacijo ključnih točk finančnega in kibernetskega sistema ter enostaven pregled interakcij med finančnim in kibernetskim omrežjem. Orodje za kibernetsko kartiranje želimo v prihodnosti nadgraditi v smeri spremljanje kibernetskega tveganja na nivoju finančnega sektorja.

Rezultate in metodologijo orodja za kibernetsko kartiranje je možno deliti z nadzorniki finančnega sektorja, odgovornimi za spremljanje operativnega oziroma kibernetskega tveganja, bodisi na mikrobonitetnim ali pa makrobonitetnem nivoju. S pomočjo kibernetskega kartiranja hitreje in bolj učinkovito spremljamo ter upravljamo s sistemskim kibernetskim tveganjem.

Z orodjem za kibernetsko kartiranje ne spremljamo samo kibernetskih incidentov, ampak tudi postopek, potreben za reševanje dogodka in potencialni vpliv na poslovanje ostalih finančnih institucij (kanali okužbe). Spremljamo lahko posredne in neposredne finančne izgube, ki jih povzročijo kibernetski napadi. Kibernetski dogodki, ki vplivajo na delovanje ključnih ekonomskih funkcij finančnega sistema, lahko spodkopavajo zaupanje v finančne institucije. Z orodjem lahko merimo nivo zaupanja (z indikatorji kot so medijska pokritost dogodka, trajanje in obseg medijske pokritosti) v bančni sistem zaradi resnih kibernetskih dogodkov.

Vzpostavitev bančnega in kibernetskega omrežja poteka postopoma, kar pomeni, da v prvem koraku pričnemo s postavitvijo bančnega omrežja. Bančno omrežje sestavljajo banke in hranilnice, ki na trgu poslujejo z gospodarstvom. Vsak subjekt na omrežju je opredeljen kot vozlišče, ki je glede na pomembnost za sistem ovrednoteno s kazalniki kot so tržni delež, število komitentov in bilančna vsota. Pomembnost kazalnika določa velikost vozlišča v sistemu, višja kot je vrednost kazalnika, bolj je subjekt pomemben

za bančni sistem. Finančne povezave ovrednotimo na podlagi medbančnega poslovanje in plačilnega prometa, s čimer dobimo pregled nad poslovanjem bančnega sektorja. Kibernetsko omrežje temelji na povezavah med tehnološkimi subjekti na trgu. Zadnji korak je povezava obeh omrežij, ki temelji na tržnem deležu IKT ponudnika, ki ponuja storitve posameznim bankam.

Ključna komponenta orodja je možnost napovedovanja strukture kibernetskega omrežja in potencialnih kibernetskih incidentov, ki bi lahko ogrozili operativno in finančno stabilnost. Napovedi temeljijo na različnih tehnikah strojnega učenja, ki nam na podlagi preteklih kibernetskih dogodkov in ostalih finančnih in drugih podatkov oblikuje bodoče kibernetsko omrežje. Napovedi kibernetskih incidentov in bodočih IKT ponudnikov so zelo natančne, saj algoritmi na podlagi preteklih dogodkov predvidevajo, kje v bančnem sistemu se bodo pojavili incidenti in povezave med bankami ter IKT ponudniki. Pri napovedovanju bodočega kibernetskega omrežja bi bilo smiselno preveriti še kakšne druge tehnike strojnega učenja, s katerimi bi lahko poskušali ocenjevati tudi izredne oziroma nepričakovane kibernetske dogodke, ki bi lahko imeli sistemski vpliv na poslovanje bančnega sektorja.

Z orodjem zaznavamo, da se na bančnem trgu tveganja koncentrirajo zaradi neposredne izpostavljenosti bank do ključnih ponudnikov IKT in oblačnih ponudnikov storitev. S pomočjo orodja spremljamo in identificiramo kritične IKT in oblačne ponudnike, skupne več bankam. Nadalje ugotavljamo, da na kritične kibernetske incidente vplivata tako neposredna izpostavljenost (poslovni odnosi med različnimi finančnimi institucijami) kot tudi posredna izpostavljenost (medsebojna povezanost različnih informacijskih sistemov ali skupnih ponudnikov storitev in operativnih sistemov). Pri tehnološki medsebojni povezanosti so problematični predvsem ponudniki tehnoloških storitev (npr. storitve v oblaku), ki lahko ob kibernetskih napadih pospešijo prenos okužbe znotraj bančnega sistema. Opažamo, da do sedaj še nismo zaznali kritičnih kibernetskih incidentov, ki bi povzročili posledice za realno gospodarstvo in bančni sektor.

Ker je nacionalna centralna banka ključna institucija v finančnem sistemu, je pomembno, da je vključena v bančno in kibernetsko omrežje. Zato je pri vzpostavljanju omrežja pomembno spremljanje finančne ter tehnološke povezave nacionalne centralne banke s poslovnimi bankami, plačilnimi ponudniki in tretjimi (zunanjimi) ponudniki storitev IKT na trgu.

6 Literatura in viri

Adelmann, F., Gaidosch, T., Morozova, A. and Wilson, C. (2019), “Cybersecurity Risk Supervision”, Departmental Paper Series, No 19/15, International Monetary Fund, Monetary and Capital Markets Department, September.

Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020), “Operational and cyber risks in the financial sector”, BIS Working Papers, No 840, Bank for International Settlements, February.

Bank of England (2021). Operational resilience: Impact tolerances for important business services. Marec 2021. Dostopno na https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf?la=en&hash=A15AE3F7E18CA731ACD30B34DF3A5EA487A9FC11.

Bank of England (2022a). Operational resilience: Impact tolerances for important business services. Marec 2022. Dostopno na https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf.

Bank of England (2022b). Prudential Regulation Authority statement on the 2022 cyber stress test: Retail payment system. December 2022. Dostopno na https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system

Banka Slovenije (2024). Poročilo o finančni stabilnosti. Maj 2024. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/fsr_april_24_03.pdf.

Borghard E. D. (2018). Protecting Financial Institutions Against Cyber Threats: A National Security Issue (september 2018). Cyber Policy Initiative Working Paper Series. Dostopno na https://carnegie-production-assets.s3.amazonaws.com/static/files/files__WP_Borghard_Financial_Cyber_formatted_complete.pdf.

Brauchle P. J., Göbel M., Seiler J. and Busekist von C. (2020). Cyber mapping the financial system. April 2020. Cyber Policy Initiative Working Paper Series. Dostopno na https://carnegie-production-assets.s3.amazonaws.com/static/files/Brauchle_Cyber_Mapping_the_Financial_System_final.pdf.

De Livera, A.M., Hyndman, R.J., & Snyder, R. D. (2011). Forecasting time series with complex seasonal patterns using exponential smoothing, Journal of the American Statistical Association, 106(496), 1513–1527. Dostopno na: https://robjhyndman.com/papers/ComplexSeasonality.pdf.

ECB (2018). Cyber resilience oversight expectations for financial market infrastructures. December 2018. Dostopno na https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

ECB (2021). “IT and cyber risk: a constant challenge”, Supervision Newsletter, 18 August.

ESRB (2020a). Systemic cyber risk. Februar 2020. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

ESRB (2020b). The making of a cyber crash: a conceptual model for systemic risk in the financial sector. Maj 2020. Dostopno na https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op16~f80ad1d83a.en.pdf

ESRB (2022). Mitigating systemic cyber risk. Januar 2022. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf.

ESRB (2023). Advancing macroprudential tools for cyber resilience. Februar 2023. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf.

ESRB (2024). Advancing macroprudential tools for cyber resilience – Operational policy tools. April 2024. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.report202404_advancingmacroprudentialtools~ca44cf0c8a.en.pdf.

Financial Stability Board (2018). Cyber Lexicon. November 2018. Dostopno na https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

IOSCO (2020), “Principles on Outsourcing”, Consultation Report, No 01/2020, May.

IMF (2020). Cyber Risk and Financial Stability: It’s a Small World After All. December 2020. Dostopno na https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622.

IMF (2024). Global Financial Stability Report. April 2024. Dostopno na https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024.

Kaffenberger L. and Kopp E. (2019). Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment (September 2019). Cyber Policy Initiative Working Paper Series. Dostopno na https://carnegie-production-assets.s3.amazonaws.com/static/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf.

Nish A. and Naumaan S. (2019). The Cyber Threat Landscape: Confronting Challenges to the Financial System (Marec 2019). Cyber Policy Initiative Working Paper Series. Dostopno na https://carnegie-production-assets.s3.amazonaws.com/static/files/03_19_Nish_Naumaan_Fin_Threats_final.pdf.

Poljšak, B. (2024a). Kibernetska varnost bančnega sistema. Ljubljana: Banka Slovenije, 2024. Dostopno na https://www.bsi.si/publikacije/raziskave-in-analize/prikazi-in-analize.

Poljšak, B. (2024b). Orodja za spremljanje sistemskega kibernetskega tveganja in prihajajoča regulativa s področja kibernetske varnosti finančnega sistema. Ljubljana : Lexpera, GV založba, 2024.

Prenio, J. and Restoy, F. (2022). Safeguarding operational resilience: the macroprudential perspective. Avgust 2022. FSI Briefs, Financial Stability Institute, Bank for International Settlements. Dostopno na https://www.bis.org/fsi/fsibriefs17.pdf.

Schonlau, M. and Yuyan Zou, R. (2020). The random forest algorithm for statistical learning. Marec 2020. The Stata Journal Volume 20, Issue 1, Pages 3-29.
Dostopno na https://journals.sagepub.com/doi/epub/10.1177/1536867X20909688.