Cyber Mapping Tool For Monitoring Of Systemic Risk

BANKA SLOVENIJE
EVROSISTEM

May 2025

Systemic cyber risk project

Project background:

- Banka Slovenije cooperated on the project with the Insurance Supervisory Agency and the Securities Market Agency. The aim of all three financial supervisors was to increase our analytical capacity for identifying and monitoring systemic cyber risk at the level of the financial system.
- The cyber mapping tool for the banking sector was one of the project results. Technical assistance for the development of the tool was provided by the IMF.
- The project started in June 2022 and was completed n September 2024.

The results of the project:

- established supervisory cyber risk database,
- cyber risk dashboard for the banking sector,
- cyber mapping tool and
- introduction of cyber resilience stress testing for banking sector.

Purpose of the tool

Cyber mapping

- is an analytical and monitoring tool that shows the key financial and technological links between financial institutions and technology service companies,
- helps supervisory authorities to identify the nodes of systemic importance and gain insight into the concentration risk and contagion channels,
- can be based on a functional or institutional approach:
  - Banka Slovenije's approach is institutional, focusing on the structure and interrelationships within the financial system. It covers two key networks: the cyber network and the financial network.
  - Alternatively, a functional approach emphasizes critical functions essential to the financial system and its stability.

The use of cyber mapping must strike a balance between the granularity of the tool and its usefulness for monitoring systemic cyber risk.

Currently, a limited number of central banks have such a tool at their disposal to monitor and identify cyber risk at the banking system level.

Objective of the tool

Cyber mapping **adds value** in the following ways:

- identification of key critical points in the financial and cyber system,
- an overview of interactions between the financial and cyber networks,
- protection of critical infrastructure at the national level,
- useful for micro-prudential and macroprudential oversight of the financial system and
- useful for managing systemic cyber risks.

The tool results in two interconnected networks

- **The cyber network** can be seen as a virtual layer of the financial network, built up from ICT components.
- By mapping **the financial network** (i.e. the financial system) to the cyber network, we can identify the links between third-party (external) ICT service providers used by financial institutions. This approach reveals information about banks that share common ICT service providers.

Mapping methodology I

Tool terminology (node definition):

Financial services entities	Central bank, banks, insurance companies, investment funds, stock brokerages
Financial infrastructure entities	Payment system operators, exchanges, CCPs, depositories, information service providers
Financial sector	All of the above
ICT entities	Hardware and software vendors, cloud service providers, telecom providers, IT service providers
ICT components	Hardware, software, networks, data centers

- **The nodes** are typically central banks, commercial banks, insurance companies, investment firms and ICT service providers.
- In defining the key nodes, it is also important to define **the map layers**, which are made up of the data flow and the organizational and technological dependencies that together form the network of links and nodes between the financial and technology sectors.
- **Data flows** between financial institutions represent either transactions or liabilities between banks, while for ICT service providers, **connections** represent the share of total outsourced ICT services provided by each ICT service provider to each bank in the market.

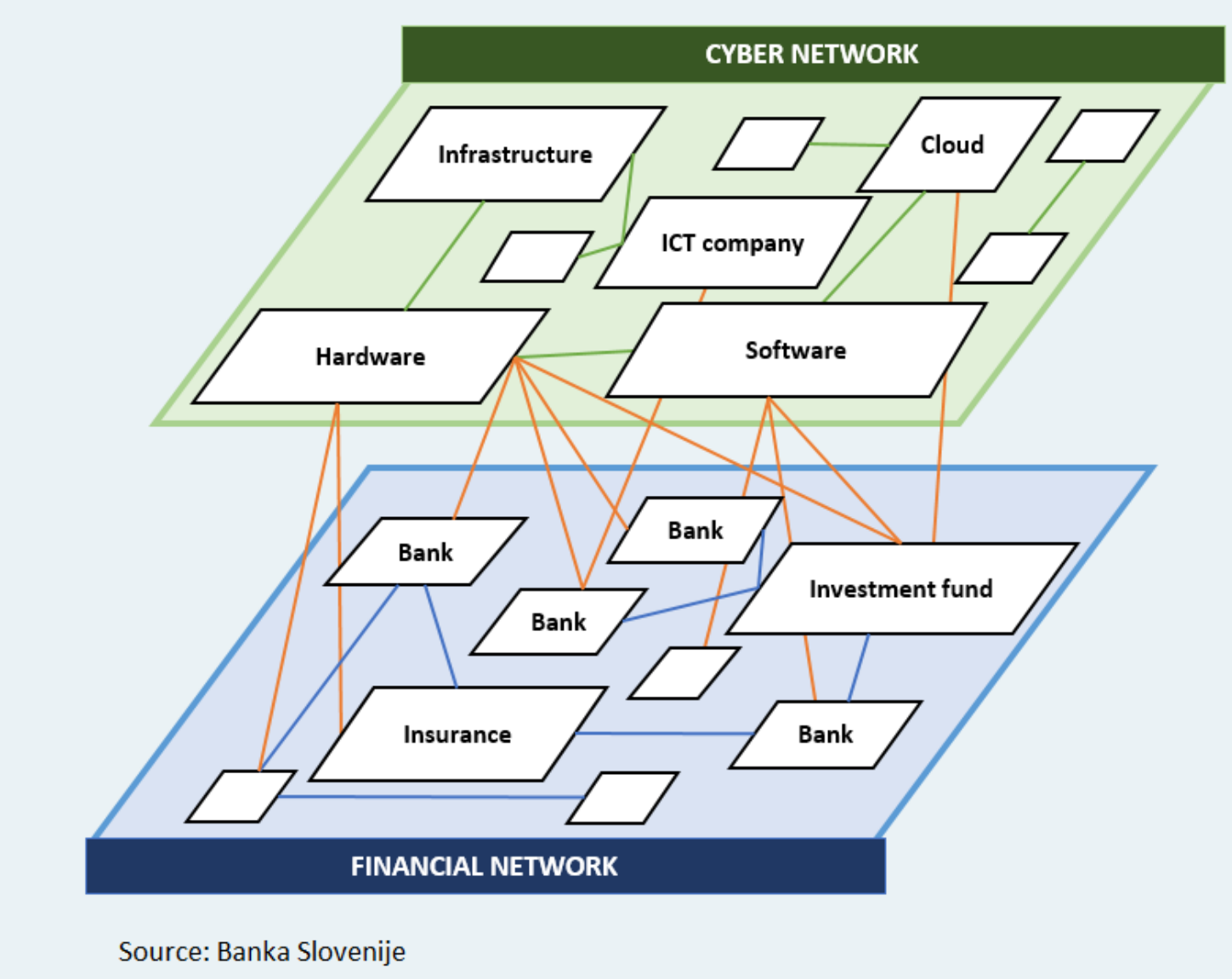
Mapping methodology II

Defining links on the map:

Layer	Showing entities	Remark
Data flows	Financial services entities Financial infrastructure entities	Focus on technical connections
Org dependencies	Financial services entities Financial infrastructure entities ICT entities	Within the financial sector Financial sector - ICT ICT – ICT
Tech dependencies	Financial services entities Financial infrastructure entities ICT entities Hardware Software Networks	Influences Org dependencies

- The nodes are further evaluated in terms of **their importance in the system** using indicators such as market share, number of customers and balance sheet total.
- We **weight** the networks of linkages between the financial and technology sectors appropriately on the basis of market shares, as this gives a more realistic reflection of risk in the banking sector.
- Cyber mapping also includes data on **cyber incidents** that have occurred in the banking system and their potential impact on the operations of other entities in the network.

Schematic illustration of the cyber map



Source: Banka Slovenije

Tool visualisation and forecast

The tool was developed using **R software** and visualized using **R Shiny.**

The result is **an app** that makes it easier to:

- monitor and identify cyber risks at the banking system level and,
- collaborate and communicate with other supervisors in case of a serious cyber event.

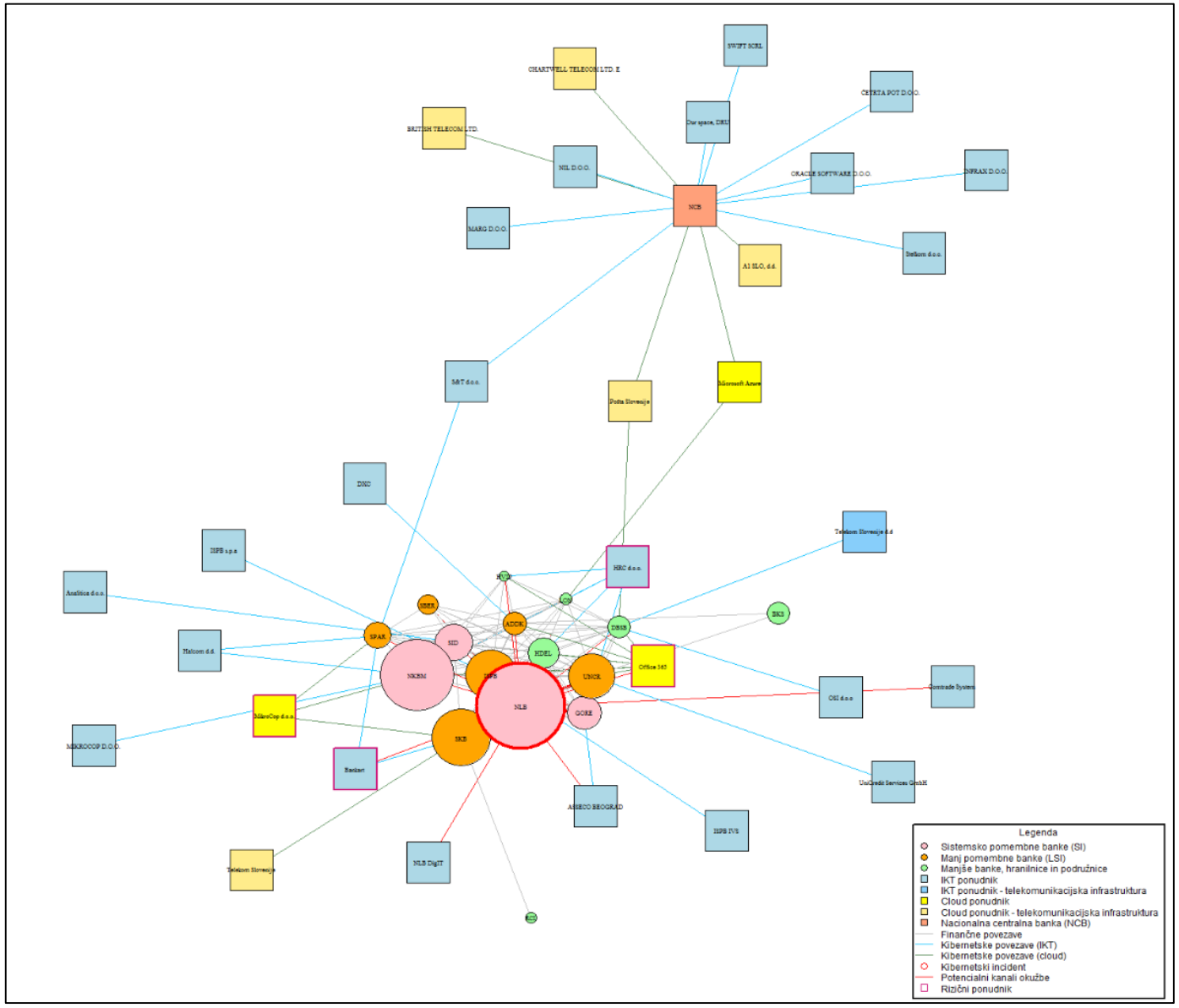
To forecast **the cyber map**, we used the TBATS technique, which is designed to forecast time series with multiple seasonal periods.

The forecast (one year ahead) shows the future links between financial sector entities, technology providers and technology solutions, as well as the potential risks in the banking system (including Banka Slovenije). This gives us a prediction of what the future systemically important nodes will be, the concentration risk and the transmission of contagion in the banking system.

Cyber risk monitoring app

Visualisation and additional functionalities:

- identifying concentrations of risk and channels of contagion,
- a map showing where cyber incidents have occurred in the system,
- a map showing the forecast for next year to see how the market will be interconnected.



Findings and conclusion

With cyber mapping tool and apps we detected:

- risks are concentrated due to **banks' direct or indirect exposure to key ICT service providers**,
- **technological interconnectedness** is particularly problematic for technology service providers (e.g. cloud services), which can accelerate the transmission of contagion within the banking system in the event of a cyber-attack,
- the Slovenian banking system is mainly confronted with cases related to **operational contagion**,
- critical cyber incidents can cause disruptions to key economic functions that are important for financial institutions to operate in the market.

We note that no critical cyber incidents with consequences for the real economy and the Slovenian banking sector have been detected so far.

Thank you for your attention!

Discussion Papers

Cyber mapping as a tool for monitoring cyber risk

Author: Borut Poljšak

October 2024

BANKA SLOVENIJE
EVROSISTEM

Collection: Discussion Papers

Title: Cyber mapping as a tool for monitoring cyber risk

Number: October 2024

Year: 2024

Place: Ljubljana

Issued by:
Banka Slovenije
Slovenska 35, 1505 Ljubljana, Slovenia
www.bsi.si

Electronic edition:

https://www.bsi.si/en/publications/research/discussion-papers

This publication is also available in Slovene.

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 212588547
ISBN 978-961-7230-04-8 (PDF)

Contents

Abstract 4

1 Introduction 5

2 Tool for monitoring systemic cyber risk 6

3 Cyber database and cyber mapping methodology 8

3.1 Cyber database 8

3.2 Cyber mapping methodology 9

3.3 Generation of the banking and cyber networks 12

3.4 Forecasting the cyber network by means of various machine learning techniques 14

4 Use of the tool for monitoring systemic cyber risk 17

5 Conclusion and next steps 21

6 References and sources 23

Abstract

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 systemic nodes by monitoring and analysing key technologies, services and connections between financial sector institutions, service providers and third-party systems. The tool is designed for both microprudential and macroprudential 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 interlinkages between different entities in the banking market.

To ensure financial stability, it is essential to have an overview of the key financial and cyber connections in the banking market. The Cyber Toolkit provides additional insight into potential contagion channels and risk concentration in the banking system. The cyber network can be considered 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 connections between the third-party ICT providers used by financial institutions.

Key words: cybersecurity, cyberattack, cyber incident, resilience, systemic risk, financial network, cyber network, financial stability, operational risk, cyber mapping

1 Introduction

Cyber risk can be defined as a combination of the probability of cyber incidents and their potential impact on banking, which might be realised in the form of operational outages, financial losses, or the transmission of risk to other sectors (Poljšak, 2024a). It is therefore vital that as supervisors of the banking sector we have at our disposal tools to monitor cyber risk. One responsibility of macroprudential policy is monitoring and mitigating systemic cyber events that could threaten the operational and financial stability of the system. Cyber mapping allows us to monitor systemic cyber risk more quickly and more effectively. This paper presents the key functionalities of a cyber mapping tool designed to monitor cyber risk at the level of the banking system or the financial system. The tool provides insight into operational and financial interlinkages between various entities in the banking market. A key feature of the tool is that it provides an overview of critical infrastructure at the national level, and makes it easier to manage systemic cyber risk (Kaffenberger & Kopp, 2019). Cyber mapping gives us an overview of the connections between financial institutions and other key entities in the banking market. This information can be used for the purpose of monitoring financial stability, and also in supervisory activities in the area of cybersecurity. Only a limited number of central banks currently have a tool of this type at their disposal to allow for the identification and monitoring of cyber risk at the level of the banking system. The more detailed the mapping is, the more expensive and time-consuming it is, particularly in the case of larger and more complex financial systems.

The tool for cyber mapping in the banking market allows us to identify the risk concentration caused by banks' direct or indirect exposure to key ICT service providers. We are aware that cyber incidents have an impact on direct exposure (business relationships between different financial institutions) and also on indirect exposure (interlinkages of different information systems or common service providers and operating systems). A successful cyberattack on a key ICT service provider could have affect on banking.

The cyber mapping tool also encompasses a forecast of the network's outlook for the year ahead. The cyber mapping forecast makes use of various machine learning techniques designed to forecast time series with multiple seasonal periods, which allow for the illustration of future financial and cyber networks. Based on past events, it is possible to generate a new cyber database and network, and to identify key connections in the system that might appear between entities in the banking sector and ICT service providers. It is also possible to forecast where in the banking system cyber incidents will occur. All the information obtained is beneficial to the ongoing monitoring of cyber risk at the level of the banking system (Poljšak, 2024b).

Cyber mapping helps supervisory authorities in identifying the main nodes of systemic importance, and in gaining insight into concentration and contagion risk. When using cyber mapping it is necessary to find a balance between granularity and utility in monitoring systemic cyber risk. The output of the tool is an illustration of two interlinked networks, namely the financial network and the cyber network. The cyber network can be treated as a virtual layer of the financial network composed of all ICT components that financial institutions use in their operations. By mapping the financial network (i.e. the financial system) to the cyber network, we can find the connections between third-party providers of ICT services used by financial institutions. This approach enables the identification of common ICT service providers (e.g. cloud providers) in the banking

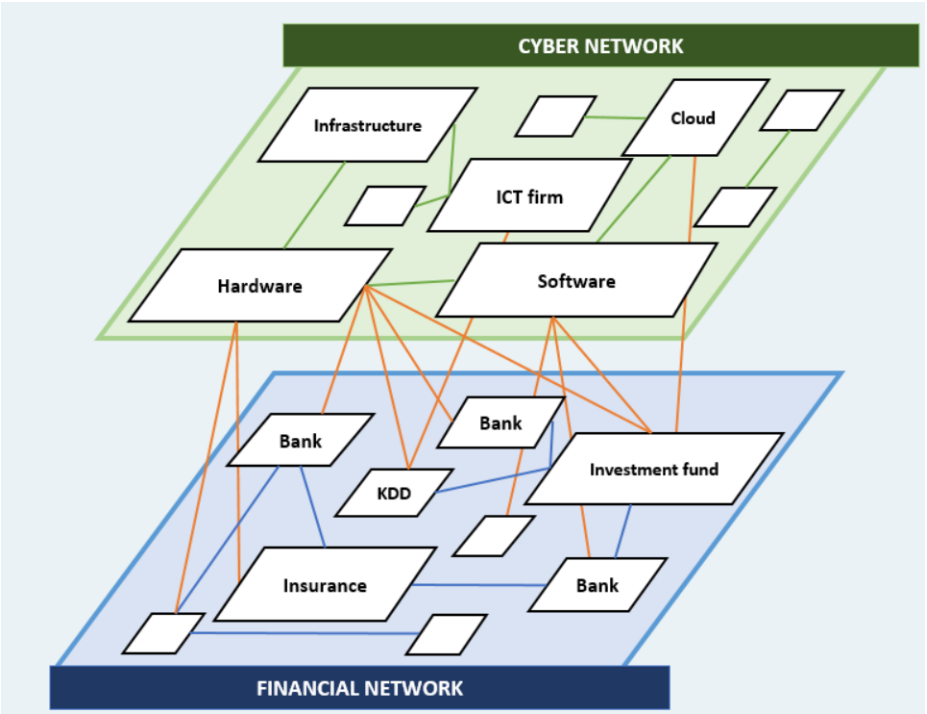
sector. This information grants financial sector supervisors oversight of risk concentration in the cyber network, and also of the contagion channels for cyber risk in the financial system (Poljšak, 2024a).

2 Tool for monitoring systemic cyber risk

In the monitoring of cyber risk, the key is that supervisors have at their disposal adequate data, indicators and information that relate to the realm of cybersecurity (ESRB, 2020a). Systemic cyber risk, which can be realised in the form of operational outages, financial damage or the transmission of contagion to other sectors, is a combination of the probability of cyber incidents and their potential impact on banking (Financial Stability Board, 2018). The key trigger of a systemic cyber event is a cyber incident that can threaten the cybersecurity of the information system and breaches the financial institution's security policy (IMF, 2020). It is therefore vital for supervisors to identify cyber risk, and also to monitor it using a tool such as cyber mapping based on a network approach (network analysis[1]).

Cyber mapping (a quantitative tool) covers the key technologies, services and external service providers, and their connections with financial sector institutions. At the conceptual level, mapping aims to highlight key financial and tech connections between financial institutions, firms and third-party technology and service providers. Cyber mapping provides an overview of financial institutions, and also the connections between financial institutions and other critical entities. To better understand the vulnerabilities and channels for the spread of contagion in the financial system, it is necessary to use cyber mapping to identify systemically important nodes at the financial and operational levels, including third-party providers (see Figure 1). This information can be used for supervision and for analysis of cyber risks to financial stability (ESRB, 2022).

Figure 1: **Schematic cyber map**



Source: Banka Slovenije

[1] Network analysis is a method of examining the relationships between entities in a network.

Figure 1 illustrates the financial connections (e.g. liabilities or payment transactions) between individual financial entities and the ICT sector, which constitutes the cyber network. The cyber network encompasses those elements of information and communication technology (ICT), such as software, hardware and communication service providers, that make up the basic infrastructure for all operational processes in the financial network (ECB, 2018 and 2021). A cyberattack on a third-party ICT service provider that provides key services for systemically important financial institutions can thus have an adverse impact on financial stability. Similar effects might be imagined in connection with software products used as common solutions across the entire financial system, which could become problematic in the event of the malfunctioning of the software as a result of a cyberattack. The resilience[2] of the cyber network is therefore vital to the stability of the financial system (Banka Slovenije, 2024).

Cyber mapping can be based on two different approaches or methodologies, as follows:

- The functional approach is based on the concept that certain functions are of key importance to the financial system and to financial stability. Under the functional approach the key critical functions are defined and classified according to the map purpose, then the institutions providing these functions are defined, together with the systems that these institutions rely on in providing the functions. Based on this map we can identify and monitor concentration risk and contagion channels in the financial system.

- The institutional approach is based on the concept that the structure of the financial sector, financial connections and processes can be linked to the cyber network. Under this approach the cyber network is treated as a virtual layer of the financial network composed of all ICT components that financial institutions use in their operations. To provide their financial services, institutions use software, hardware and other ICT components provided by ICT service providers (third parties). By mapping the financial network (i.e. the financial system) to the cyber network, we can identify the connections between the key third-party ICT service providers used by systemically important financial institutions. This approach enables the identification of common ICT service providers (e.g. cloud providers) in the financial sector. This tool also allows financial sector supervisors to identify concentration risk[3] in the network and the contagion channels for the transmission of cyber risk to the financial system.

Banka Slovenije has developed cyber mapping based on the institutional approach. We opted for this approach because our banking system and tech market are smaller compared with larger EU countries, and a tool based on this approach is not too complex from the perspective of maintenance. Cyber mapping provides for the following forms of added value for the supervisory monitoring of cyber risk:

- identifying key points in the financial system and the cyber system,
- overseeing interactions between financial and cyber networks,
- protecting critical infrastructure at the national level, and
- managing systemic cyber risks.

[2] Cyber resilience can be defined as the capacity of a bank or any other financial institution to realise its mission statement through the anticipation and management of cyber risks, and fast recovery from cyber incidents.

[3] Concentration risk arises from banks' large exposure to certain ICT service providers. This risk could be realised in the event of a bank being unable to operate normally or provide key economic functions as a result of the unavailability of a key ICT service provider.

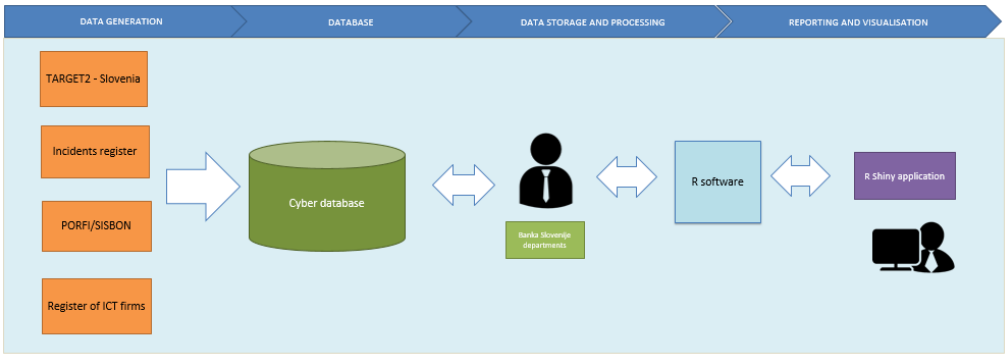
3 Cyber database and cyber mapping methodology

Before developing a cyber mapping tool it is necessary to create a cyber database and set out the methodology based on which the financial and cyber networks will be generated. The cyber database encompasses not only data about ICT service providers and reports of cyber incidents, but also financial data from individual supervised entities. This database forms the basis for the development and functioning of a cyber mapping tool based on the institutional approach.

3.1 Cyber database

To develop a cyber mapping tool we need data on domestic payments and settlements (located in the TARGET2 system), and financial data on banking (reporting by financial institutions and SISBON). Thy cyber database contains data on total assets, market share, earnings, mutual claims between banks, capital and bank customers. Two registers have been created for the needs of generating the cyber network. The first register encompasses the reports of cyber incidents submitted to the central bank by reporting banks. These reports contain key data and information about the incident's impact on banking. The second register encompasses a list of all ICT service providers that provide services to banks.

Figure 2: **Architectural concept of the system**



Source: Banka Slovenije

Figure 2 illustrates the data flow for the transmission of financial and cyber data into the cyber database. The data can be accessed either directly by accessing the database, or via pre-prepared supervisory and statistical reports designed for monitoring cybersecurity in the banking sector. The supervisory and statistical reports encompass key operational and financial indicators that signal systemic cyber risk at the level of the banking system. The cyber database is also the basis for developing the cyber mapping tool and application.[4]

The output of the cyber mapping tool can be shared with a large number of supervisors who are responsible for monitoring operational risk and cyber risk, either at the microprudential or macroprudential level (Borghard, 2018).

[4] The cyber mapping tool was developed using R software, while the visualisation tool was developed using R Shiny.

3.2 Cyber mapping methodology

Cyber mapping begins by taking a bird's eye view of the financial sector. Identifying systemically important institutions in the financial sector is a prerequisite for analysing any destabilising influences on the financial network from the cyber network. A successful cyberattack hitting just one of these systemically important actors could develop into a direct threat to the financial system as a whole (Bank of England, 2022a).

A cyberattack on a critical number of non-systemically important entities could also pose a risk to operational and financial stability (ESRB, 2020b). It is not necessary for this critical mass to consist solely of entities in a single sector. Hacker groups might carry out a cyberattack on a group of heterogenous institutions who belong to different sectors, but who all use the same software or the same ICT service provider in the cloud. Although the financial system can be divided into individual sectors, it is also necessary to address cyber risk from an intersectoral perspective (Bank of England, 2021). The financial and cyber networks must therefore include institutions that are important to the functioning of the banking system, and that could threaten financial stability in the event of disruption caused by cyberattacks (see Table 1).

Table 1: **Institutions of importance to the functioning of the banking system**

Sector	Systemic importance
Banks	Banks are classified according to their importance in the banking system, namely as systemically important banks, less significant banks, and savings banks and branches. In the event of a successful cyberattack on a systemically important institution, this could also affect the operations of other banks in the system.
Financial infrastructure	Financial infrastructure plays a key role in the functioning of the banking system, as it allows for the accounting and settlement of payments (TARGET2), securities and derivatives (KDD), and other financial transactions (Bankart).
National central bank	The central bank is the most important financial institution in the network; its non-functioning would lead to the non-functioning of the financial system.
ICT service providers	The key ICT service providers are those providing services to significant financial institutions. The non-functioning of common ICT service providers could pose a threat to banking.
Cloud service providers	More and more banks are using the services of cloud providers. This is increasing their exposure, and the risks to banks should cloud services be unavailable as a result of cyberattacks. An even larger problem arises if multiple banks depend on the same cloud provider.
Other sectors	Entities providing services to systemically important financial institutions, and whose operations could be impacted in the event of disruptions (intersectoral impact).

Source: Banka Slovenije

Not every cyberattack on a systemically important institution in the financial network has a systemic impact, but each nevertheless poses a potential cyber threat to financial stability (IMF, 2024). This depends above all on which key economic functions the cyberattack hits, and how long the operational outage lasts (Bank of England, 2022b). The cyber mapping tool shows where in the financial system cyber incidents have occurred, and how they directly or indirectly impacted other systemically important institutions in the financial and technology networks.

The cyber mapping tool is used to monitor and identify:

- Which financial institutions a cyber incident occurred in, the recovery time needed to resolve the event, and the potential impact on the operations of

other financial institutions (contagion channels). On this basis we can identify whether the financial institution that was subject to a cyberattack is capable of ensuring business continuity. The plan addresses events that pose a major risk of operational outage, and usually includes a secondary or backup location.

- Systemically important disruptions as a result of a cyber event (any operational outage of a systemically important institution or their key economic functions that would not be resolved by the end of the business day). The identification of past events of this kind allows for faster action in the event of an actual incident, which could prevent the development of a systemic event that might threaten the operations of financial institutions.

- The contagion channels for transmitting the cyber shock to the entire financial system, and the potential financial losses as a result of the cyber event. We can monitor the direct and indirect financial losses caused by cyberattacks.

- Cyber events that impact the working of the key economic functions of the financial system can undermine confidence in financial institutions, which is difficult to measure and assess. The assessment of the impact of a cyber event on public confidence in the financial system is therefore primarily qualitative in nature. The impact on confidence in the financial system can be measured by the following indicators: media coverage of the event, and the duration and scope of media coverage (for example inter-regional or international). These factors can create the impression of a potentially destabilising impact from a cyber event via the confidence channel.

Table 2: **Entities on the map**

Terminology	Description
Financial service entities	Central banks, banks, insurance corporations, investment funds, investment firms
Financial infrastructure entities	Payment system operators, stock exchanges, repositories, information service providers
Financial sector	All of the above (financial service entities and financial infrastructure entities)
ICT entities	Hardware and software vendors, cloud service providers, telecommunications service providers, IT service providers
ICT components	Hardware and software, networks, data centres

Source: Banka Slovenije

The first step in developing the tool is defining nodes. Nodes are usually central banks, commercial banks, insurance corporations, investment firms and ICT service providers. In defining the key nodes it is important to also define the map layers made up of data flow and organisational and technological dependencies that together form the network of nodes and connections between the financial sector and the tech sector (see Table 2). The data flow between financial institutions consists of either transactions or liabilities between banks, while for ICT service providers the connections represent the share of all ICT services provided by ICT service providers that the individual ICT service provider provides to the individual bank in the market. Nodes are additionally evaluated in terms of systemic importance by means of indicators such as market share, number

of customers, and total assets. The network of connections between the financial sector and the tech sector is appropriately weighted by market share, thereby yielding a more realistic picture of risk in the banking sector. Cyber mapping also includes data about critical cyber incidents that have occurred in the banking system, and their potential impact on the operations of other entities in the network.

Table 3: **Cyber mapping terminology (identification of nodes)**

Level	Entities illustrated	Note
Financial connections	Entities subject to financial supervision	Focus on tech connections
	Financial infrastructure	
Organisational dependence	Financial service entities	In the financial sector
	Financial infrastructure	Financial sector (ICT)
	ICT entities	ICT to ICT
Tech dependence	Financial service entities	Impact of organisational dependence
	Financial infrastructure	
	ICT entities	
	Hardware	
	Software	
	Network	

Source: Banka Slovenije

The cyber network encompasses all ICT elements that make up the basic infrastructure for all operational processes taking place in the financial network. The key technical elements of ICT infrastructure are hardware, software and built-in devices used to operate applications software (Brauchle et al., 2020). The provision of banking services of this kind is increasingly being outsourced to third-party ICT service providers (see Table 3).

The key components of the cyber network and the risks in connection with cyberattacks are as follows:

- Software: the overwhelming majority of cyberattacks are undertaken by means of malware, which hackers use to infiltrate and damage information systems.

- Hardware: hardware can be manipulated, for instance, by modifying it using additional structural components, changing existing circuits, tampering with chips, or modifying firmware. Tampering with ATMs, point-of-sale systems, and credit cards are examples of hacker infiltrations. Centralised computer centres used by multiple banks can pose increased concentration risk.

- Cloud computing: the majority of cloud service providers provide similar services to numerous financial institutions. When a large number of financial institutions depend on a single cloud service provider, concentration risk can arise. A successful cyberattack on a cloud service provider could harm service availability, and threaten data confidentiality or integrity.

- ICT outsourcing: a growing number of financial institutions are outsourcing their services to ICT service providers, which is increasing their exposure should there be a major cyberattack on the provision of a key economic function that is also supported by third-party ICT service providers. Major cyberattacks could

lead to computer centres or ATMs ceasing to work for a certain amount of time (IOSCO, 2020).

All of these key ICT components are captured and illustrated in the cyber network, and are connected directly or indirectly to the financial institutions that together make up the cyber network. A cyberattack on one of the key ICT components could cause the outage of services of importance to banks and their customers. It is therefore vital that banks and savings banks have business continuity plans in place (Nish & Naumaan, 2019).

3.3 Generation of the banking and cyber networks

The generation of the banking and cyber networks is undertaken gradually, which means that the first step is the generation of the banking network. The banking network consists of the banks and savings banks transacting with the economy in the market. Banks are classified with regard to their importance to the banking system as follows: (i) systemically important banks, (ii) less significant banks and (iii) savings banks and branches. The next step is to further define the importance of the individual bank in the banking system. Each market entity is defined as a node, which is evaluated in terms of its importance in the system via indicators such as market share, number of customers, and total assets. The importance indicator determines the size of the node in the system: the higher the indicator, the more important the entity is to the banking system. Evaluating the nodes allows us to identify the key entities that need to be interconnected into the banking network in the next step. The banking network consists of financial connections based on the settlement of mutual domestic payments and liabilities between banks. The financial connections yield an overview of the banks' financial operations, the opportunities for contagion, and the risk concentration in the event of a major cyberattack.

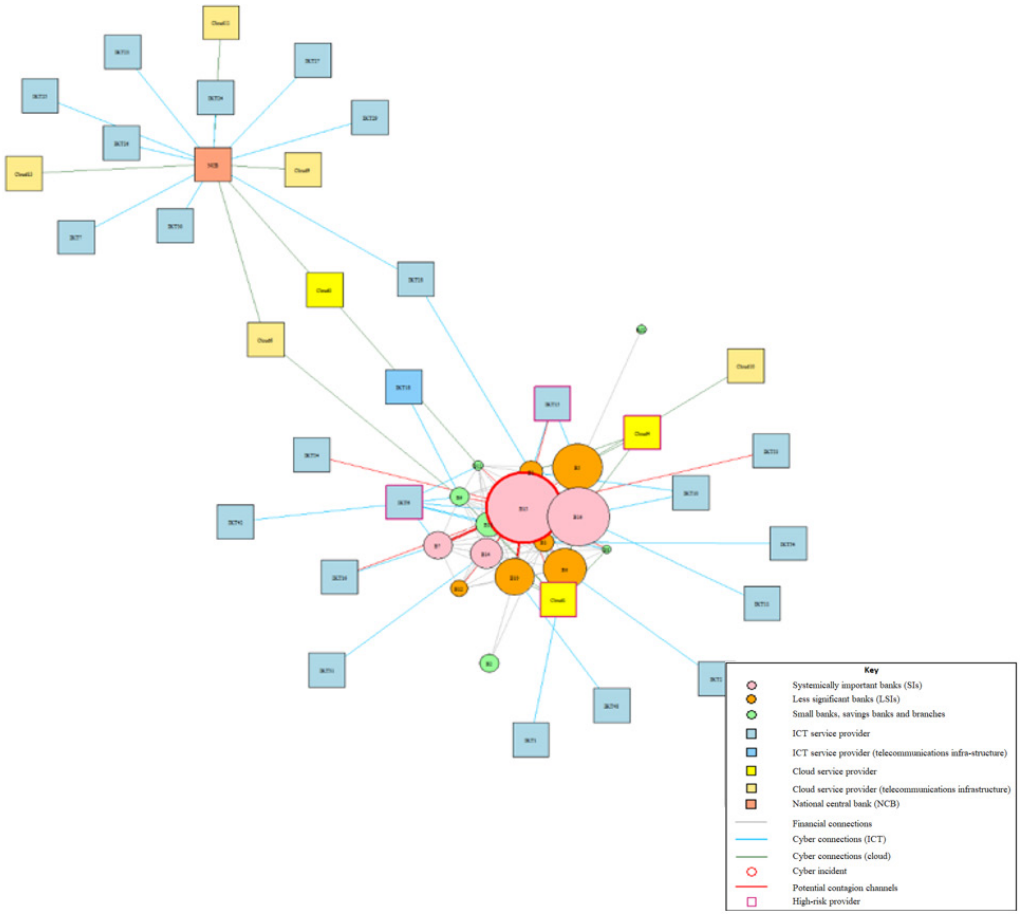
Once the banking network has been generated, it is time for the generation of the cyber network, which is based on the connections between various tech entities in the market. These are various third-party ICT service providers (including cloud services and telecommunications services). The cyber network solely illustrates the key tech entities that provide ICT services to the banking sector. The connections between tech entities in the market are determined on the basis of business cooperation. This means that particular ICT firms order services such as hardware, software or cloud services from other ICT firms.

The key connections between tech entities make up the cyber network, which is extremely interlinked and interdependent. This means that a successful cyberattack could hit specific tech firms providing specific tech services to banks, which could cause an outage of specific information systems supporting banks. It is therefore vital that the connections between the banking network and the tech network are illustrated on the map. These connections need to be appropriately weighted, for example by market share,[5] which allows for a more realistic picture of the impact of a cyber incident on the functioning of the banking sector and the tech sector. Using these weights, the most important tech entities in the network are disclosed, which allows banking sector supervisors to focus on the key vulnerabilities in the system.

[5] The data flow between financial institutions consists of transactions or liabilities between banks, while at ICT service providers it is the individual provider's share of all services of third-party ICT service providers for a particular bank in the market. The nodes are additionally evaluated in terms of systemic importance by means of indicators such as market share, number of customers, and total assets.

The cyber network also includes data on cyber incidents that arose and occurred in both the banking sector and the tech sector, and their potential impact on the operations of other entities in the cyber network. Information about past major cyber incidents is also vital for forecasting where incidents can be expected in the future in the banking network and the tech network. Incidents are marked in red in both the banking network and the cyber network. The generation of the banking network and the cyber network and the interlinkages (between banks, between tech entities, and between banks and tech entities) provide a comprehensive overview of the third-party ICT service providers used by banks in their operations. The cyber network helps us to see that there are third-party ICT service providers in the market who provide similar services to multiple banks. The generation of the banking network and the cyber network makes it easier for supervisors to monitor risk concentration in the system, and also the contagion channels for the transmission of cyber risk into the banking system (see Figure 3).

Figure 3: **Banking and cyber networks**



Source: Banka Slovenije

Because the national central bank is the key institution in the financial system, it is important to include it in the banking network and the cyber network. In generating the networks it is important to monitor the national central bank's financial and tech connections with commercial banks, payment service providers and third-party ICT service providers.

3.4 Forecasting the cyber network by means of various machine learning techniques

The cyber mapping tool also encompasses a forecast of the network for the year ahead. Various machine learning techniques were used in forecasting the future cyber network. These techniques are based on forecasting time series designed to estimate future values on the basis of values determined in the past. The first technique for forecasting a cyber map was TBATS, a method designed to forecast time series with multiple seasonal periods. TBATS is a forecasting method for modelling data series whose main objective is forecasting time series with complex seasonal patterns using exponential smoothing (see Table 4). The forecast (for one year ahead) illustrates future connections between financial sector entities, tech providers and tech solutions, and potential risks in the banking system (including Banka Slovenije), thereby identifying future systemically important nodes where concentration risk is present and the potential for contagion in the banking system.

The TBATS technique uses various methods of exponential smoothing, and can be described by the following equations:

Table 4: **Description of TBATS technique**

Model	Description of model
$y_t^{(\lambda)} = l_{t-1} + \Phi b_{t-1} + \sum_{i=1}^{T} s^{(i)}_{t-mi} + d_t$	$y_t^{(\lambda)}$ = time series at time t $s_t^{(i)}$ = i^{th} seasonal component
$l_t = l_{t-1} + \Phi b_{t-1} + \alpha d_t$	l_t = local level
$b_t = \Phi b_{t-1} + \beta d_t$	b_t = trend with damping
$d_t = \sum_{i=1}^{p} \varphi_i d_{t-1} + \sum_{i=1}^{q} \Theta_i e_{t-1} + e_t$	d_t = ARMA(p, q) process and residuals e_t = Gaussian white noise process
Seasonal component	**Model parameters**
$s_t^{(i)} = \sum_{j=1}^{(k_i)} s^{(i)}_{j,t}$	T – size of seasonality m_i – length of i^{th} seasonal period
$s^{(i)}_{j,t} = s^{(i)}_{j,t-1} \cos(\omega i) + s^{*(i)}_{j,t-1} \sin(\omega_i) + \gamma_1^{(i)} d_t$ $s^{*(i)}_{j,t} = -s^{(i)}_{j,t-1} \sin(\omega i) + s^{*(i)}_{j,t-1} \cos(\omega_i) + \gamma_2^{(i)} d_t$	λ – Box-Cox transformation α, β – smoothing parameters Φ – damping parameter
$\omega_i = 2 \pi j / m_i$	φ_i, Φ_i – ARMA[6] (p, q) coefficients $\gamma_1^{(i)}$, $\gamma_2^{(i)}$ – seasonal smoothing (two for each period)

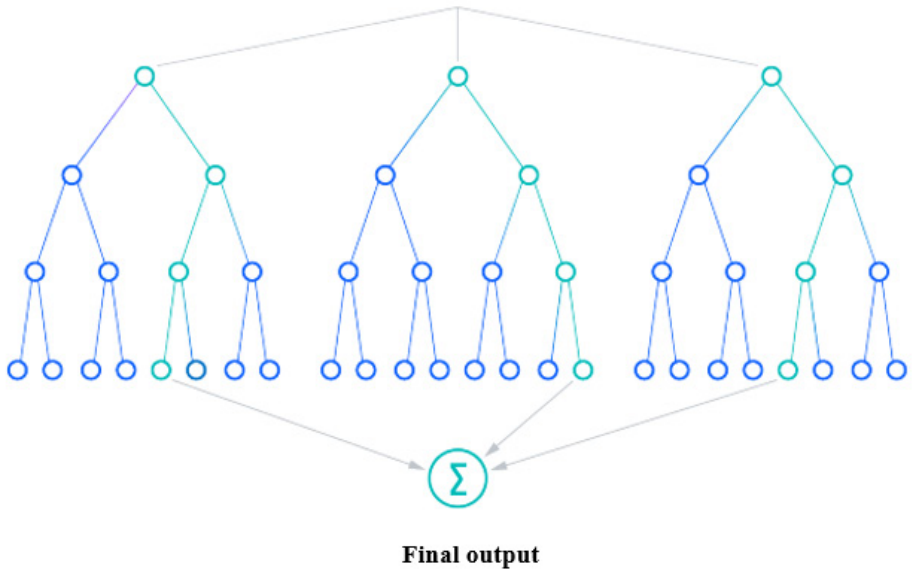
Source: De Livera et al., 2011

The second technique used for forecasting is based on a random forest algorithm. It uses a machine learning algorithm that combines the results of multiple decision trees into a single result that provides the basis for forecasting the future cyber network (Schonlau et al., 2020). The random forest algorithm is based on three parameters that need to be set before learning: node size (number of customers, total assets), number of trees (banks, ICT service providers) and number of sampled properties (transactions, liabilities, operations between banks and ICT service providers). The random forest classifier is then used to tackle the regression or classification problems. The random forest algorithm consists of a set of decision trees, where each tree in the set is built

[6] In the statistical analysis of time series, autoregressive-moving-average (ARMA) models are a way to describe a stationary stochastic process using two polynomials, one for autoregression and one for moving average.

from data samples taken from the learning dataset with replacement, known as a bootstrap sample (see Figure 4).

Figure 4: **Forecasting by means of decision forests**



Source: Banka Slovenije

The final result represents a forecast of future connections between financial sector entities, tech providers and tech solutions, and the potential cyber risk in the banking system and the tech sector. Forecasting by means of random decision trees is based on learning from past events and also from past forecasts, thereby driving a continual improvement in the forecasts of the future cyber network over time.

The third machine learning technique used for forecasting is based on support vector regression. It is used for forecasting time series, share prices in particular, and also cyberattacks and other potential risks in the operations of financial institutions. The aim of support vector regression is to find a function that predicts a continuous target variable, and in so doing identifies the difference between the forecast values and the actual data points. Support vector regression determines a range around the forecast regression line, and aims to adjust the line inside this range, thereby minimising the forecasting error. In support vector regression the data points that are closest to the regression line and that determine the difference are known as support vectors. These points play a key role in determining the regression model. Support vector regression tries to find a regression model with a range around the forecast values that provides a balance between fitting to the data and avoiding overfitting. It is particularly useful in the treatment of non-linear relationships, where the choice of kernel function can help it adapt to various problem areas, including forecasting the future cyber network and potential risks to the banking sector caused by major cyber incidents.

The forecasts of the future cyber map from the individual machine learning techniques were also tested on past data. The machine learning techniques provide forecasts of total assets, the number of customers (corporate and retail), market share, the occurrence of cyber incidents, and payment transactions for the year ahead. The deviations in the forecasts from the actual values ranged from 6% to 10% at the level of the banking system. There is variation in the deviations under each of the aforementioned techniques, which means that it is sensible to use a combination of all three machine learning techniques in the forecasting, which improves the forecasting probability.

The forecasts of cyber incidents and future ICT service providers are very accurate, as the algorithm based on past events predicts where in the banking system incidents will occur, and the connections between banks and ICT service providers. The machine learning techniques provide forecasts of the following financial data: total assets, the number of corporate and retail customers who hold accounts at banks, bank market shares, and the number of critical cyber incidents reported to the central bank by commercial banks. The forecast includes data on domestic payments and information about ICT service providers. On the basis of the results from the machine learning techniques described above, the deviations in the forecasts from the actual values were estimated, and were classified into four categories (see Table 5).

Table 5: **Comparison of forecasts under various machine learning techniques**

Bank	Total assets			Number of retail customers			Number of corporate customers			Market share			Cyber incidents		
	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%
SYSTEM	6%	4%	6%	1%	1%	0%	2%	10%	11%	5%	5%	7%	0%	3%	0%

Colour code		
	Very accurate forecast	Deviation from actual value is less than 5%
	Good forecast	Deviation from actual value is between 5% and 10%
	Reasonable forecast	Deviation from actual value is between 11% and 20%
	Inaccurate forecast	Deviation from actual value is more than 20%

Source: Banka Slovenije
Note: TBATS: technique for forecasting time series with multiple seasonal periods. RF: random forest. SVR: support vector regression for forecasting time series.

The best forecast of the future cyber network was given by the TBATS technique. The deviations in the forecast from the actual values amount to just over 4% at system level, the technique thus providing a very accurate forecast. The results in the forecasting of future cyber incidents are even better: the deviation from the actual number is just 1%.

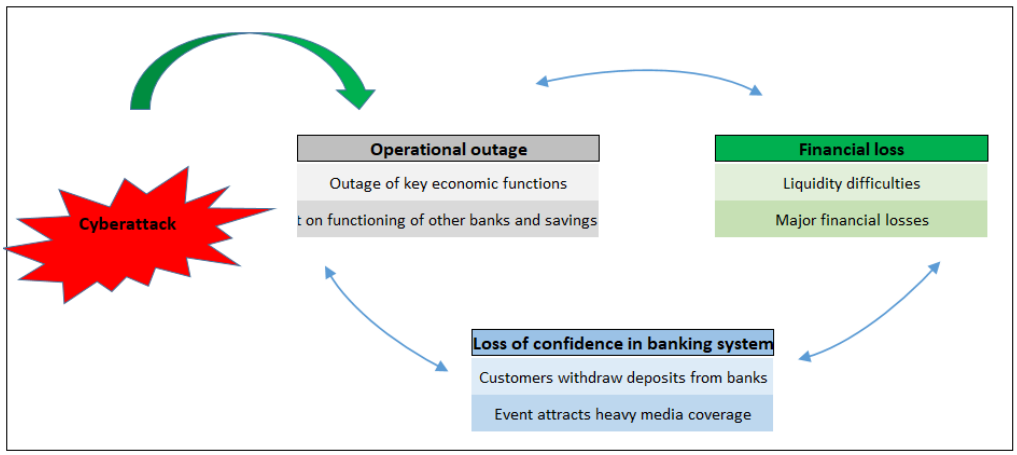
The techniques based on the random forest algorithm and on support vector regression return slightly worse results: the deviations from the actual values range from 5% to 6% at system level, which nevertheless represents a good forecast.

4 Use of the tool for monitoring systemic cyber risk

The cyber mapping tool is designed to monitor and identify cyber vulnerabilities at the level of individual banks, and at the level of the banking system. From the perspective of financial stability and macroprudential policy, our interest lies in the systemic effects of an individual cyberattack on the banking system (Prenio & Restoy, 2022). The impact of a cyberattack on financial stability is monitored from three perspectives: (i) the operational working of key economic functions, and the transmission of any outage to other banks, (ii) the size of the financial losses (in connection with the duration of any long-term outage of key economic functions), and (iii) the loss of confidence in the banking system. We monitor how cyber incidents impact the operations of the individual bank, other banks, and third-party ICT service providers that provide services to banks (see Figure 5).

The tool is used to monitor the direct and indirect financial losses of key economic functions at the level of individual banks and at the level of the banking system. If a cyberattack disrupts the functioning of key operations for a substantial time, this entails loss of access to financial assets and the ability to settle liabilities, as a result of which parties to transactions and market participants lose confidence in the banking system. If the event has heavy media coverage, this could have a major impact on public confidence in the banking system, which makes it vital for banks to run appropriate media campaigns aimed at restoring public confidence in the banking system.

Figure 5: **Impact of cyberattack on financial stability and potential contagion channels in the banking system**



Source: Banka Slovenije

The next important information that can be obtained using the tool is monitoring potential contagion channels in the banking system. The tool is used to monitor two types of potential contagion that can appear in the banking system as a result of a cyberattack, namely operational contagion and financial contagion.[7] A cyberattack first hits the operational functioning of banks and ICT firms, which can trigger operational contagion. This means that the outage of key economic functions at one bank affects the working of economic functions at other banks, and also affects the common ICT service providers supporting the functioning of core bank information systems. Disruptions to these systems could in turn affect the operations of other banks not impacted directly.

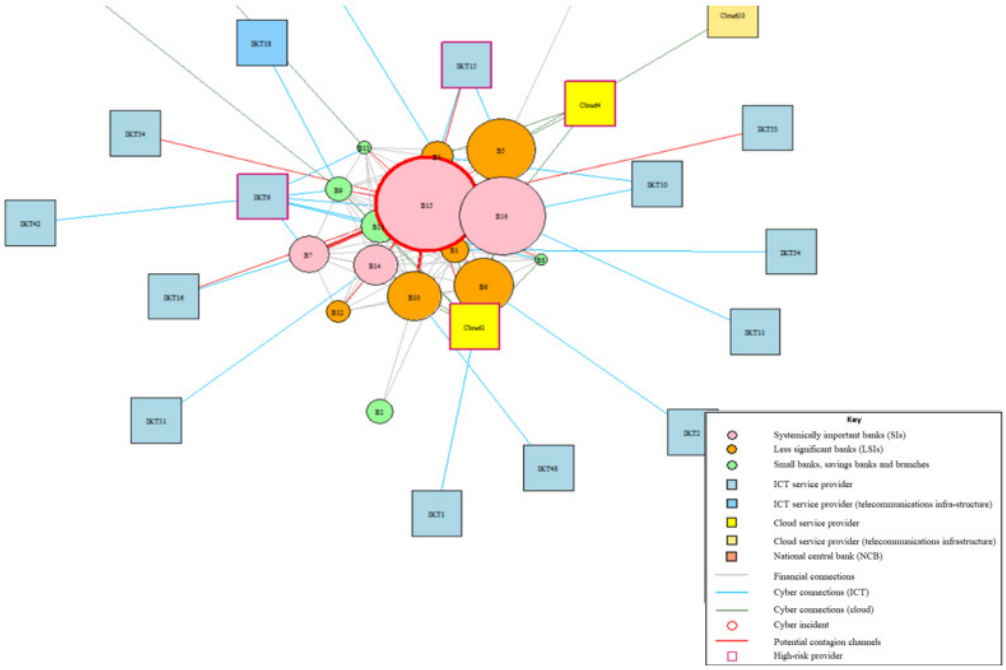
[7] Financial contagion might be defined as a stress event that hits the banking sector as a result of interlinkages, fire sales on financial markets, or illiquidity. The source of contagion can therefore be just an individual component of the banking system, whose problems for example might affect interbank operations.

A longer outage of bank information systems at a large number of banks could lead to operational contagion. The tool can quickly identify operational contagion in the network by monitoring each critical cyber incident that might affect interbank operations, or the functioning of other bank information systems or common ICT service providers. The tool can also assess the operational stability of the banking system,[8] which can be endangered by critical cyber incidents.

The longer that key economic functions and core bank information systems do not work, the greater is the impact on financial losses and the liquidity of the banking system. This also increases the potential for financial contagion in the system, which could lead to financial instability. While direct financial losses are mainly caused by the loss of commission from the non-functioning of payments and the costs associated with recovery, the indirect losses relate to the materialisation of reputation risk.

The indirect financial loss caused by a major cyberattack on the banking system can be measured by the number of customers lost, the related loss of income, and the costs of media campaigns aiming to restore the reputation of the bank and the banking system. In the event of sustained operational instability, a major cyberattack could impact the liquidity of the banking system and funding risk. The tool monitors and measures how individual cyber incidents might lead to the withdrawal of sight deposits, and thus to a decline in net income, at individual banks and also at the level of the banking system. This identifies the potential risks with regard to the settlement of liabilities (payments and cash operations).

Figure 6: **Potential contagion channels and funding risk in the banking system**



Source: Banka Slovenije

Operational and financial contagion can also affect other entities in the financial and tech markets. Should key ICT service providers be unable to operate in the market as a result of a cyberattack, this could affect the operations of particular banks and insurance corporations, and the capital market. Potential contagion channels arise in these situations, which the tool can identify, thus making it easier for banking supervisors to

[8] Operational stability relates to the ability of banks to maintain their operations without disruptions to key economic functions that might be caused by cyberattacks.

take action and to communicate with other supervisors (the ISA[9] and the SMA[10]) and with the Government Information Security Office.

We find that risks in the banking market are concentrated by banks' direct exposure to key ICT service providers and cloud service providers. The tool can identify and monitor common critical ICT and cloud service providers providing information services to banks. This means that a major cyberattack on a common ICT or cloud service provider could affect the provision of ICT services to specific banks. Should a key ICT service provider be unable to provide information services to banks, this would also affect the operations of the banking sector and the economy. The tool makes use of an algorithm to classify the key ICT service providers of importance to the operations of the banking sector.

There is an awareness that cyber incidents have an impact on direct exposure (business relationships between different financial institutions) and also on indirect exposure (interlinkages of different information systems or common service providers and operating systems). A successful cyberattack on a key ICT service provider could affect banking. Banks who order their IT solutions and support from external providers and suppliers might be more exposed to cyberattacks and cyber incidents (Aldasoro et al., 2020). The main issue with tech interlinkages is providers of tech services (e.g. cloud services) who during cyberattacks can speed up the transmission of contagion within the banking system. Based on the identified critical cyber incidents, we observe that the banking system mainly faces cases of operational contagion.

The cyber mapping tool also encompasses a forecast of cyber indicators for the year ahead. The tool can be used to forecast the key operational and financial indicators in connection with the cybersecurity of the banking sector outlined in Table 6.

[9] Insurance Supervision Agency.
[10] Securities Market Agency.

Table 6: **Forecast of key cyber indicators**

Indicator	Description	Note
Number of critical cyber incidents reported	Number of critical cyber incidents reported to the central bank	Commercial banks are required to report cyber incidents to the central bank on the basis of the EBA guidelines defining the reporting criteria.
Estimate of indirect financial loss	The monetary loss indirectly caused by the incident (e.g. costs of compensation for damage to customers, potential judicial costs).	Unilateral risk. A higher value for this indicator entails potentially greater structural systemic risk.
Estimate of direct financial loss	The monetary loss directly caused by the incident, including those losses incurred by the rectification of the incident (e.g. expropriated assets or funds, costs of replacing hardware and software, penalties for non-performance of contractual obligations).	
Share of all reported cyber incidents in Slovenia accounted for by banking	This indicator provides information about how much the banking sector is exposed to cyber incidents compared with other sectors.	
Share of all reported cyber incidents that are critical	This indicator provides information about how many cyber incidents are critical compared with the total number of reported incidents.	
Number of phishing and DDoS attacks	The most common types of cyberattack on commercial banks are phishing and DDoS, for which reason they are forecast on the basis of past trends.	
Share of IT budget spent on security	The indicator measures how much of their total IT budgets (development, outsourcing, infrastructure, etc.) banks earmark for IT security.	
Number of devices with obsolete software	Obsolete software increases the information vulnerability of individual banks and the banking system.	

Source: Banka Slovenije

Based on the forecasts for individual indicators, we can monitor risks in the area of cybersecurity at the level of the banking system. The tool can also predict potential malicious activities by internal and external agents. These forecasts can make it easier to take action aimed at strengthening the banking sector's cyber resilience.

5 Conclusion and next steps

In a time of rapid digitalisation and globalisation of the financial sector, the supervisory monitoring and identification of potential cyber threats is vital (Adelmann et al., 2019). One tool that allows us to do so is cyber mapping, which is aimed at financial sector supervisors, and is designed to make it easier to monitor cyber risk and to take action on this basis, once the threats that could jeopardise the operational and financial stability of the banking system have been identified. The cyber mapping tool can be defined as a tool for managing the information that is vital to the management of future cyber crises by financial sector supervisors (ESRB, 2023). The tool is the key to collecting, processing and redistributing information about major cyber events (ESRB, 2024). It also aims to provide information about major cyber events to individual banks and other supervisors at the sectoral and intersectoral levels alike (see Figure 6).

The tool and the additional visualisation can be used to quickly discern the key financial connections between individual financial entities and the ICT sector that constitutes the cyber network. The cyber network covers all elements of information and communication technology that make up the basic infrastructure for all operational processes in the financial network. On this basis we developed a cyber mapping tool based on an institutional approach. This approach is based on the idea that the structure of the financial sector, financial connections and processes can be linked to the cyber network. We opted for this approach because the banking system and the tech market are smaller in Slovenia compared with large EU countries, and are not overly complex from the perspective of maintenance. Cyber mapping brings added value for financial sector supervisors by allowing them to identify key points of the financial and cyber systems, and giving them a simple overview of the interactions between the financial network and the cyber network. The aim is to upgrade the cyber mapping tool in the future in the direction of monitoring cyber risk at the level of the financial sector.

The output and methodology of the cyber mapping tool can be shared with the financial sector supervisors who are responsible for monitoring operational risk and cyber risk, either at the microprudential or macroprudential level. Cyber mapping allows us to monitor systemic cyber risk more quickly and more effectively, and to manage systemic cyber risk.

The cyber mapping tool is used to monitor not only cyber incidents, but also the process needed to recover from the event and the potential impact on the operations of other financial institutions (contagion channels). We can monitor the direct and indirect financial losses caused by cyberattacks. Cyber events that impact the working of the key economic functions of the financial system can undermine confidence in financial institutions. The tool can be used to measure the level of confidence (through indicators such as media coverage of an event, duration and scope of media coverage) in the banking system following major cyber events.

The generation of the banking and cyber networks is undertaken gradually, which means that the first step is the generation of the banking network. The banking network consists of the banks and savings banks transacting with the economy in the market. Each entity in the network is defined as a node, which is evaluated with regard to its importance to the system by means of indicators such as market share, number of customers and total assets. The importance indicator determines the size of the node in the system: the higher the indicator, the more important the entity is to the banking system. Financial connections are evaluated on the basis of interbank operations and

payments, thus yielding an overview of the operations of the banking sector. The cyber network is based on connections between entities in the tech market. The final step is connecting the two networks, which is based on the market shares of ICT service providers providing services to individual banks.

A key component of the tool is the ability to forecast the structure of the cyber network and potential cyber incidents that could jeopardise operational and financial stability. The forecasts are based on various machine learning techniques, which are used to generate a future cyber network on the basis of past events and other financial and non-financial data. The forecasts of cyber incidents and future ICT service providers are very accurate, as the algorithm based on past events predicts where in the banking system incidents will occur, and the connections between banks and ICT service providers. In forecasting the future cyber network it would be wise to examine any other machine learning techniques that might try to assess extraordinary or unexpected cyber events that could have a systemic impact on banking.

The tool recognises that risks in the banking market are concentrated by banks' direct exposure to key ICT service providers and cloud service providers. The tool can be used to identify and monitor critical ICT service and cloud service providers common to multiple banks. We further find that critical cyber incidents are affected by direct exposure (business relationships between different financial institutions) and also by indirect exposure (interlinkages of different information systems or common service providers and operating systems). The main issue with tech interlinkages is providers of tech services (e.g. cloud services) who during cyberattacks can speed up the transmission of contagion within the banking system. We should note that so far we have not identified any critical cyber incidents that would have consequences for the real sector and the banking sector.

Because the national central bank is the key institution in the financial system, it is important to include it in the banking network and the cyber network. In generating the networks it is therefore important to monitor the national central bank's financial and tech connections with commercial banks, payment service providers and third-party ICT service providers in the market.

6 References and sources

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. March 2021. Available at: 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. March 2022. Available at: 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. Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system

Banka Slovenije (2024). Financial Stability Review. May 2024. Available at: https://bankaslovenije.blob.core.windows.net/publication-files/fsr_april_24_en_l.pdf

Borghard, E.D. (2018). Protecting Financial Institutions Against Cyber Threats: A National Security Issue (September 2018). Cyber Policy Initiative Working Paper Series. Available at: 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 Von Busekist, C. (2020). Cyber mapping the financial system. April 2020. Cyber Policy Initiative Working Paper Series. Available at: https://carnegie-production-assets.s3.amazonaws.com/static/files/Brauchle_Cyber_Mapping_the_Financial_System_final.pdf

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

ECB (2018). Cyber resilience oversight expectations for financial market infrastructures. December 2018. Available at: 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. February 2020. Available at: 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. May 2020. Available at: https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op16~f80ad1d83a.en.pdf

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

ESRB (2023). Advancing macroprudential tools for cyber resilience. February 2023. Available at: 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. Available at:
https://www.esrb.europa.eu/pub/pdf/reports/esrb.report202404_advancingmacroprudentialtools~ca44cf0c8a.en.pdf

Financial Stability Board (2018). Cyber Lexicon. November 2018. Available at: 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. Available at: 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. Available at:
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. Available at: 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 (March 2019). Cyber Policy Initiative Working Paper Series. Available at: https://carnegie-production-assets.s3.amazonaws.com/static/files/03_19_Nish_Naumaan_Fin_Threats_final.pdf

Poljšak, B. (2024a). Cybersecurity of the banking system. Ljubljana: Banka Slovenije, 2024. Available (in Slovene) at: https://www.bsi.si/publikacije/raziskave-in-analize/prikazi-in-analize

Poljšak, B. (2024b). Tools for monitoring systemic cyber risk and upcoming regulation in the area of the cybersecurity of the financial system. Ljubljana: Lexpera, GV založba, 2024.

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

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