6-1-2024

Exploring Cybertechnology Standards Through Bibliometrics: Case of National Institute of Standards and Technology

Tugrul Daim
Portland State University

Haydar Yalcin
Ege University

Alain Mermoud
Armasuisse Science and Technology

Valentin Mulder
Armasuisse Science and Technology

Citation Details

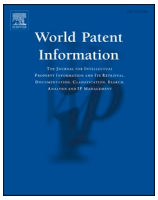
Daim, T., Yalcin, H., Mermoud, A., & Mulder, V. (2024). Exploring cybertechnology standards through bibliometrics: Case of National Institute of Standards and Technology. World Patent Information, 77, 102278.

World Patent Information 77 (2024) 102278

Contents lists available at ScienceDirect

World Patent Information

journal homepage: www.elsevier.com/locate/worpatin



Exploring cybertechnology standards through bibliometrics: Case of National Institute of Standards and Technology☆

Tugrul Daim [a,b,1,*], Haydar Yalcin [a], Alain Mermoud [c], Valentin Mulder [c]

[a] Ege University, Erzene Mahallesi Ege Universitesi Merkez Yerleşkesi, 35040, Bornova, Izmir, Turkey
[b] Portland State University, Portland, OR, USA
[c] Cyber-Defence Campus, armasuisse Science and Technology, EPFL Innovation Park, Lausanne, Switzerland

ARTICLE INFO

Keywords:
Technology analysis
Techmining
Social network analysis
Cybersecurity
National institue of standards and technology

ABSTRACT

Cyber security is one of the topics that gain importance today. It is necessary to determine the basic components, basic dynamics, and main actors of the Cyber security issue, which is obvious that it will have an impact in many areas from social, social, economic, environmental, and political aspects, as a hot research topic. When the subject literature is examined, it has become a trend-forming research subject followed by institutions and organizations that produce R&D policy, starting from the level of governments. In this study, cybersecurity research is examined in the context of 5 basic cyber security functions specified in the cyber security standard (CSF) defined by the National Institute of Standards and Technology (NIST). It is aimed to determine the research topics emerging in the international literature, to identify the most productive countries, to determine the rankings created by these countries according to their functions, to determine the research clusters and research focuses. In the study, several quantitative methods were used, especially scientometrics, social network analysis (SNA) line theory and structural hole analysis. Statistical tests (Log-Likelihood Ratio) were used to reveal the prominent areas, and the text mining method was also used. we first defined a workflow according to the "Identify", "Protect", "Detect", "Respond" and "Recover" setups, and conducted an online search on the Web of Science (WoS) to access the information on the publications on the relevant topics It is seen that actors, institutions and research create different densities according to various geographical regions in the 5 functions defined within the framework of cybersecurity. It is possible to say that infiltration detection, the internet of things and the concept of artificial intelligence are among the other prominent research focuses, although it is seen that smart grids are among the most prominent research topics. In the first clustering analysis we performed, we can say that 17 clusters are formed, especially when we look under the definition function. The largest of these clusters has 32 data points, so-called "decision making models".

1. Introduction and background

Cybersecurity can be defined as a discipline that focuses on securing computer systems, networks, software, and data. We can say that they aim to protect against cyber-attacks, prevent unauthorized access, ensure data confidentiality, ensure data integrity, and make information systems useable at all levels [1–3]. Cyber security applications appear to consist of several sub-components. While the component that includes the work done for the protection of computer networks is called network Security, it covers topics such as protecting network components (router, switch, firewall, etc.), monitoring and filtering traffic, removing network weaknesses, and taking precautions against attack [4]. In system security, which includes studies to ensure the security of information systems such as operating systems, servers, desktop computers and mobile devices, issues such as authentication, access control, security patches, detection and prevention of malicious software are examined [5]. In data security, which aims to ensure the security of sensitive and personal data, solutions are developed for issues such as data

☆ This research was funded by armasuisse Federal Office for Defence Procurement; contract number 8203005331.
* Corresponding author. Portland State University, Portland, OR, USA.
E-mail address: tugrul.u.daim@pdx.edu (T. Daim).
https://www.linkedin.com/in/tugruldaim (T. Daim), https://www.linkedin.com/in/haydar-yal%C3%A7in-6bb9a527 (H. Yalcin), https://www.linkedin.com/in/alainmermoud (A. Mermoud), https://www.linkedin.com/in/valentin-mulder (V. Mulder)
[1] Tugrul Daim was a visiting faculty at Ege University during this research project.

https://doi.org/10.1016/j.wpi.2024.102278
Received 29 June 2023; Received in revised form 10 March 2024; Accepted 5 April 2024
Available online 20 April 2024

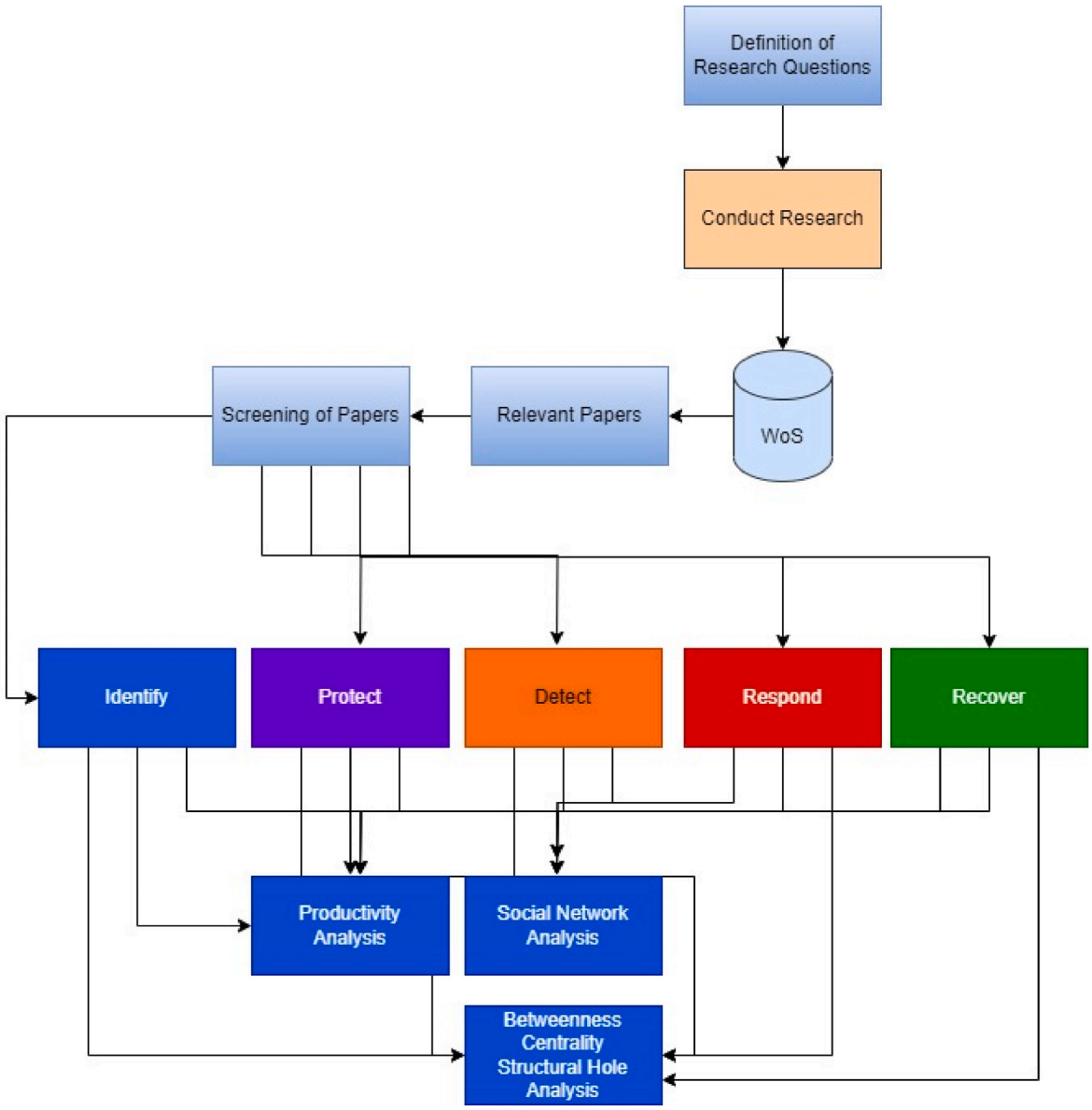


Fig. 1. Study workflow.

encryption, database security, data recovery and backup, and data loss prevention [5–7]. In the studies carried out to ensure the security of applications defined as Software Security, topics such as secure software development, detection of weak points, security tests and code analysis are covered [8,9]. Cryptography can also be shown among the topics sought for solutions in this context: Investigating the methods of encrypting and decrypting information, Cryptography is used to provide confidentiality, integrity and authentication in communication [10,11]. Finally, there comes the Social Engineering applications, which is a unit that examines an area where attackers try to access sensitive information by manipulating people. While dealing with social engineering, psychology, and human behavior, it aims to produce solutions for applications that aim to deceive users with methods such as giving information, phishing, and fraud [12,13]. Since the issue of cyber security has the potential to affect many areas in terms of social, economic, environmental, and political aspects, it has been a subject discussed at the level of governments [14,15]. Looking at the literature, previous studies indicate that in many situations where the corporate world lives, organizations have permeable controls on attack detection and monitoring, incident response, or IT forensics. Although it is stated that cyber problems can originate from internal and external sources of any organization or system, it requires organizations to do internal research as well as focus on external interaction in parallel with the world trend. For organizations to better combat attacks, they need to look both internally and externally and establish a solid cybersecurity stance against potential attackers, regardless of which vector originates. In the UK, the Center for Conservation of Critical National Infrastructure (CPNI) defines Critical National Infrastructure (KUA) as follows: the facilities, systems, sites, and networks that enable the country to function socially and economically and provide essential services needed to sustain everyday life in England [16,17]. In a world where 80 percent of private sector industries operate national assets as part of their core business, there is a compelling need for better understanding, protection and maintenance of critical assets and information infrastructures against cyber threats [18]. There is limited consumer and end-user understanding or technical skills against growing cyber threats [19–21]. The USA, which aims to produce solutions according to the principles of multiple perspective analysis, has also carried out a series of studies on this subject. Focusing on five main functions from the main reference points of the subject, the USA aimed to develop a standard based on

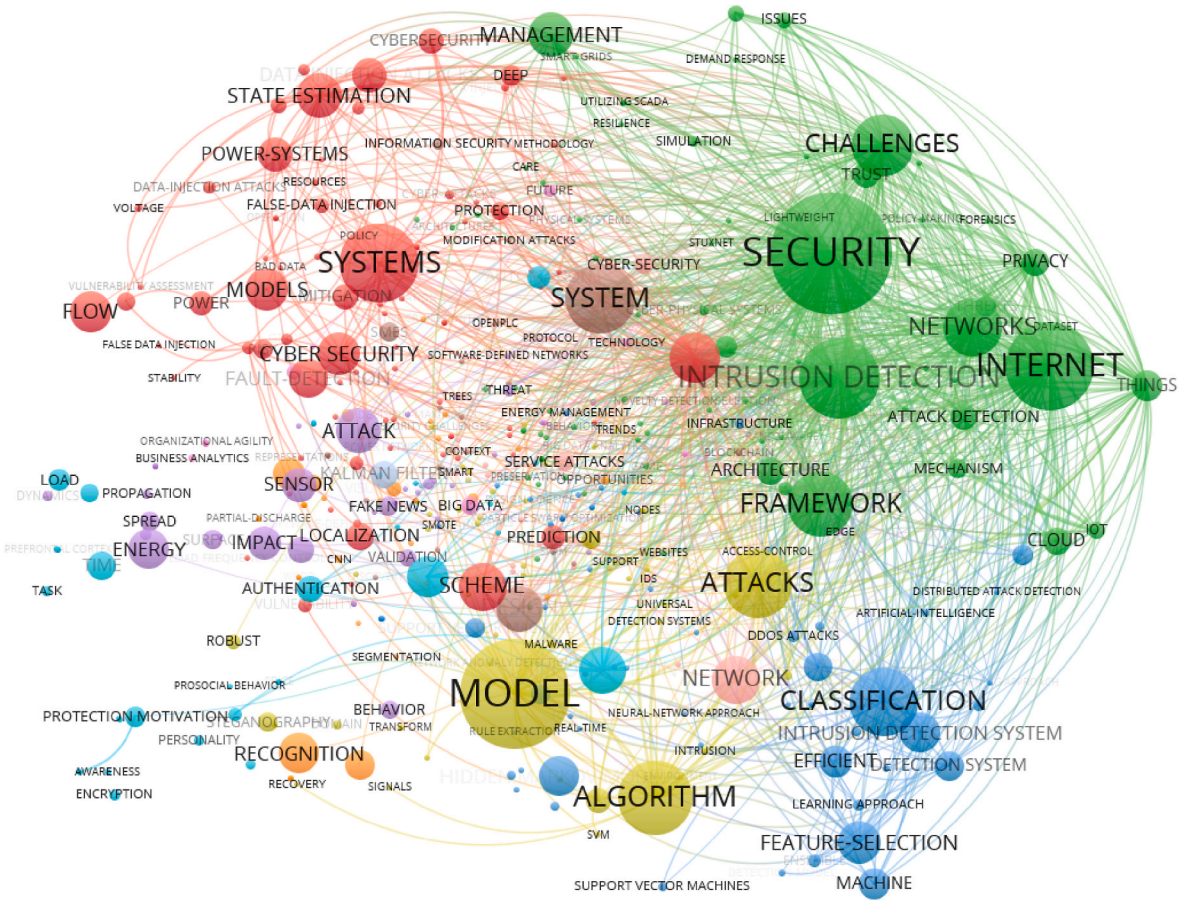


Fig. 2. Keyword analysis.

these functions. Since the subject consists of so many sub-components and application areas, it has become necessary to develop a standard on this subject and a framework consisting of five basic functions has been developed for cybersecurity. The responsibility of the work to be done for this purpose has been undertaken by the American Standard Institute called National Institute of Standards and Technology (NIST). NIST is a federal agency that provides standards and guidance on science, technology, and cybersecurity systems in the United States [22, 23]. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) has been developed to determine applicable security standards and rules in all industries with critical infrastructure. NIST CSF aims to provide a flexible and repeatable structure based on performance and efficiency, while helping to identify, assess and manage cyber risks. In this respect, it can be said that it aims to identify improvement areas for existing cyber risks, to identify security gaps that are not met by published standards, and to develop action plans for these gaps [24]. NIST has developed several frameworks (frameworks) in the field of cybersecurity, one of which is called the NIST Cybersecurity Framework (NIST Cybersecurity Framework). Since our study will be based on this framework, we believe that it will be useful to give information about the subject. The NIST Cybersecurity Framework is a guide to help those concerned manage their cybersecurity risks and improve their security programs. The framework consists of five main functional categories.

1. **Identify**: It is designed to help organizations understand cybersecurity risks, identify their assets and storage, create their risk strategy, and perform an organizational-level security assessment.
2. **Protect**: It includes security measures such as raising awareness of cyber security, access control, secure network design, system configuration.
3. **Detect**: Helps organizations set up protection strategies to help detect cyberattacks or security incidents and quickly identify cybergroups. It includes operations such as reporting of detection observations of events, log management, and threat intelligence monitoring.
4. **Respond (Reply)**: Helps organizations respond to cybersecurity groups quickly and effectively to direct attacks. This process, which includes operations such as emergency management, incident management, intrusion detection and prevention, and intervention against the application, is very important.
5. **Recover**: Helps organizations plan and perform normal business process reassembly after cybersecurity incidents. It includes operations such as data backup and recovery, system restore, business continuity.

The NIST Cybersecurity Framework highlights the principle of "Continuous Improvement," a cycle to enable organizations to continually improve their cybersecurity practices.

2. Methodology

At the set of our research, we intended to explore both journal publications [25,26] and patents [27–29] to explore the research and development activity in different clusters of cybersecurity as defined by NIST. This approach is very common in literature [30]. Unfortunately, there was not a critical number of patents found in individual clusters. However prior literature [31,32]. demonstrate that journal paper trends

are good early indicators of IP trends. Therefore, we made conclusions about expected IP trends based on bibliometric trends. Since the standards are new, patenting should already be in process in this field. We expect the patenting to follow publications closely in the coming months or a year or two.

We then defined a workflow according to the “Identify”, “Protect”, “Detect”, “Respond” and “Recover” setups, and conducted an online search on the Web of Science (WoS) to access the information on the publications on the relevant topics (Fig. 1).

In the next stage, we performed productivity analysis and social network analysis (SNA) applications. In SNA analysis, we examined the indicators required to detect developing (LAC) and mature (HAC) points, especially with structural hole analysis. We revealed the differences between nodes with high constraint aggregate and nodes with low constraint aggregate. By looking at the betweenness centrality values within the scope of SNA over the centrality values, we have ensured that the nodes are ranked according to the importance of their roles in the network [33] (Fig. 2). Productivity analysis includes several elements, including examining the number, citations, publication process, and impact of a researcher’s or an institution’s publications [34]. In our study, indicators such as the number of articles published by the researcher or institution in a certain period, the number of citations of published articles by other researchers, the performance of the researcher or institution in academic indexes were examined. With the social network analysis, the actors with the highest degree of connectivity (degree), the actors with the highest betweenness centrality value, the actors with high constraint rate and the nodes with low constraint rate were examined [35–38]. Each social network analysis indicator is ranked for the five functions (identify, protect, detect, respond, and recover) determined by NIST for the cybersecurity field. In this way, the rankings obtained have made it possible to identify the prominent actors for each function, the actors acting as a bridge, the actors that have strengthened their network position, and the actors that are open to development and will increase in relative importance. To give brief information about the analyzes made, it can be said that he made a series of evaluations based on the basic indicators based on Social Network Analysis. If we explain the values we examined in this context: With Degree Partition, it is aimed to calculate the indicators expressing the number of connections of each term with other terms in the network. In this way, the centrality degree of the term, which is the number of edges (connections) coming to the node (term) in the network [10]. With the Betweenness Centrality indicator, we planned to measure the extent to which a term acts as a bridge or intermediary between other terms in the network. In this regard, by measuring the number of shortest paths passing through the term, it was possible to identify the terms with the highest potential for information flow or impact [37]. We calculated a series of indicators for the detection of virgin areas by structural hole analysis. In this context, we first took a closer look at the Low Aggregate Constraints (LAC): indicator. According to this indicator, which expresses the degree to which the terms and neighboring terms are related to each other, a low LAC value indicates that the neighboring terms of a term are not strongly related to each other. In this respect, it is possible to say that the terms with this value indicate that they have less restrictions in terms of information flow or interaction between their neighbors, while they refer to relatively untouched or developing nodal points. It is possible to detect nodes that have strengthened their position in the network with the High Aggregate Constraints Constraint (HAC) value. In other words, the HAC value, which is the opposite indicator of the LAC value, expresses the extent to which a term is related to its neighboring terms, while a high HAC value indicates that the term has a high restriction in terms of information flow or interaction between its neighbors. Considering the SNA values obtained, it is possible to make the following inferences about the terms in the field of cybersecurity [38].

Cluster analysis stands out as an analysis method that is increasingly used as one of the main methodologies of choice for analyzing multivariate data [39,40]. In our study, we aimed to group research focuses by using the clustering function to better understand Cybersecurity research and identify prominent research focuses, so that we can identify cybersecurity clusters within the years when they formed critical cohesion. While this gave us the opportunity to see the dynamics of research focuses that have emerged in the field of cybersecurity over the years, it has given us the opportunity to closely follow the basic dynamics of the field by showing how far the research clusters have diverged from each other [41].

If we are to describe the metrics for each cluster, we see that the largest cluster (Cluster 0) stands out from the others with 24 data points and a high silhouette score of 0.935. The label associated with this cluster (LLR) is "Attack detection" and the data points in this cluster are The average year is 2017 (751.85, 1.0E-4). Cluster 1 has 16 data points with a silhouette score of 0.852. It has been labeled as "Human cybersecurity behavior" according to this cluster (LLR) algorithm, where good similarity was detected between data points within the cluster. Cluster 2 is labeled "Data breaches" and the average year of data points in this cluster is 2015. Cluster 3 is identified by the label "Supply chain management" with 16 data points, while the average year of data points in this cluster is 2016.

It can be said that the clusters represent different topics or themes within the dataset based on the label associated with each cluster. On the other hand, the silhouette score for each cluster indicates the similarity of the data points within the cluster, while the higher scores indicate higher similarity. The average year of data points in each cluster provides information about the time or period in which the research related to the subject of the cluster was conducted. In general, these metrics can be translated into important inputs that can be used in policy making with information about the clustering patterns and characteristics of the data points in each cluster.

2.1. social network analysis

2.1.1. NIST’s identify

Aiming to guide the development of organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities, this function is the basis for the effective use of NIST’s cybersecurity framework. This Function, Asset Management, aims to understand the business context, the resources that support critical functions, and the associated cybersecurity risks, enabling organizations to focus and prioritize their efforts consistent with their risk management strategy and business needs; business environment; Management; Risk assessment; and Outcome Categories such as Risk Management Strategy [42–44].

If we compare the clusters according to the parameters in the table; It is observed that the sizes of the clusters vary between 11 and 32, while the largest cluster, Cluster 0, has 32 data points. Clusters 16 and 17 have the smallest cluster sizes. The average year associated with each cluster represents the temporal direction. The clusters cover a year range from 2015 to 2017 with varying distributions. Cluster 0 has 32 data points and shows a concentration for the topic of “modelling decision-making” in 2016. In other words, it is possible to say that there is a trend that shows a significant focus on understanding and managing the risks associated with decision-making in context of cyber security. Cluster 1, with its 30 data points, represents the concept of “vulnerability assessment” that emerged around 2016. It represents a crucial research focus in that it demonstrates a focus on the application of vulnerability assessment, potentially aimed at improving cybersecurity services. Cluster 2 represents the set of 30 data points labeled as “anti-malware behavior”. This cluster, which represents research or discussions about people or techniques that reached critical density in 2016 and plays a critical role in hacking or cybersecurity, is one of the prominent research focuses for NIST’s Identify function. On the other hand, it is observed that the focus is on “smart factory” consisting of cluster 3 and 30 data points. A group of 30 data points that are strongly associated with the concept of smart factories. These data points likely reflect research,

Table 1
Summary of the largest 18 clusters (Identify).

ClusterID	Size	Silhouette	Label (LLR)	Average Year
0	32	0.79	modelling decision-making (178.19, 1.0E-4)	2016
1	30	0.818	vulnerability assessment (165.42, 1.0E-4)	2016
2	30	0.882	anti-malware behaviour (202.92, 1.0E-4)	2016
3	30	0.866	smart factory (178.28, 1.0E-4)	2017
4	27	0.939	exploratory study (204.51, 1.0E-4)	2015
5	25	0.89	incident response (205.66, 1.0E-4)	2017
6	25	0.888	cyberattack detection (212.24, 1.0E-4)	2019
7	24	0.935	using deep learning (676.17, 1.0E-4)	2017
8	24	0.938	future research (274.99, 1.0E-4)	2015
9	23	0.99	smart grid (781.72, 1.0E-4)	2016
10	21	0.921	blockchain technology (344.89, 1.0E-4)	2017
11	21	0.983	managerial perspective (206, 1.0E-4)	2018
12	19	0.942	cyber risk (255.14, 1.0E-4)	2017
13	17	0.933	autonomous vehicle (192.8, 1.0E-4)	2017
14	14	1	weakests link (257.41, 1.0E-4)	2016
15	13	0.88	virtual reality environment (186.42, 1.0E-4)	2016
16	11	0.976	5g network (249.99, 1.0E-4)	2017
17	11	0.946	data breaches (247.95, 1.0E-4)	2017

discussions, or data related to the implementation, technologies, and advancements in smart factories during the year 2017. The silhouette values that emerged in the clustering analysis show that although the clusters are well separated from each other, they are located very close to each other in terms of neighborhood relations. The prominent clusters for the identify function and the indicators that are the basis for cluster analysis are given in Table 1 and Fig. 3.

2.1.2. NIST's protect

Aiming to guide the development and implementation of appropriate measures to ensure the secure delivery of critical infrastructure services, this function helps limit or contain the impact of a potential cybersecurity incident. According to NIST, the output categories included in this function are Access Control; Awareness and Education; Data security; Information Protection Processes and Procedures; Care; and Protective Technology processes [22,45].

The cluster has the largest size with 0.27 data points (Fig. 4). Cluster 14 has the smallest size with only 7 data points. Silhouette Coefficient: The 10th, 12th, and 13th clusters have the highest silhouette coefficient of 1 Cluster 2 has the lowest silhouette coefficient of 0.773, which can be interpreted as indicating some overlap or less distinctiveness between the data points. When the label is compared in terms of Average Year, it can be interpreted that the average years have changed from 2013 to 2019, in other words, the time frames in which the research focuses are interested or relevant are concentrated in this six-year period. To summarize, it is clearly seen that the clusters differ in size, silhouette coefficient, subject and average year of prominence. According to the results of the cluster analysis, the topics represented by the tags, "security assessment methodologies", "vulnerability risks", "technological research", "critical infrastructure", "secure data transmission", "behavioral strategies", "technology adoption", "cybersecurity" " is shaped as "cyber-physical security" (Table 2).

2.1.3. NIST's detect

The Detection Function, which includes developing and implementing appropriate activities to identify the occurrence of a cyber security incident, aims to ensure that cyber security incidents are discovered at the time they occur. This Function is Abnormalities and Events; Security Continuous Monitoring; and Results Categories such as Detection Actions [22,46].

When we compare clusters, it can be said that cluster 2 is the largest cluster with 28 data points (Fig. 5), while Cluster 16 is the smallest cluster with only 6 data points in terms of cluster size. When we evaluate it within the framework of the silhouette coefficient, it is possible to say that the quality of the cluster is at a good level. Cluster 8 is labeled "DDoS Attack" and Cluster 11 is "Automated Cyber". The average year for most clusters is 2018, suggesting that research or data points in these clusters are relatively new. In general, "cybersecurity", "energy internet", "Internet of Things", "artificial intelligence", etc. It covers a range of topics such as Clusters are tabulated with details showing varying sizes, silhouette coefficients, thematic focuses, and publication years, reflecting the diversity and complexity of the research field (Table 3).

2.1.4. NIST's respond

Aimed at developing and implementing appropriate actions to take on a detected cybersecurity incident, the Response Function as a function aims to support the ability to contain the impact of a potential cybersecurity incident. Respond Function Response Planning; Communication; Analysis; Decrease; and Improvements [47,48].

If we compare clusters (Fig. 6), it is seen that cluster sizes vary according to the number of data points they contain. Cluster 0 has the largest size with 18 data points, while Clusters 5, 6, 7, 8 and 9, 10 and 11 represent the smallest clusters in terms of the number of data points they contain. The silhouette coefficient measures the compactness and separation of clusters. Cluster 7 stands out with its high silhouette coefficient of 0.98, which indicates that the data points within the cluster are well separated from the other clusters. The LLR method was used to identify a tag representing the dominant theme or topic within each cluster. Accordingly, its tags can be said to provide insights into the main focus areas in each cluster. In this respect, it is possible to say that the 1st Cluster is labeled as "Classification Measure" and the 4th Cluster "Reinforcement Learning".

While the average year represents the temporal direction of the clusters, it denotes the average publication year of the data points in each cluster. In this regard, it is seen that the research focuses on the respond function have average years ranging from 2015 to 2020. By looking at this value, it can be said that the studies on the respond function are a mixture of recent and relatively old research points (Table 4).

2.1.5. NIST's recover

The recover function, which refers to developing and implementing appropriate activities to maintain resilience plans and restore capabilities or services that have been disrupted due to a cybersecurity incident, supports timely recovery of normal operations to mitigate the impact of a cybersecurity incident. This Function is Recovery Planning; Improvements; and Communication results categories [49,50].

When we compare these clusters, it is seen that Cluster 0 is the largest with 10 data points, and Clusters 8 and 9 are the smallest with 4 and 3 data points, respectively. Cluster 1, which is the second largest cluster, is labeled "False Data Injection Attack", while Cluster 6 is labeled "Railway Communications Case Study". When we want to represent the temporal direction of the clusters in terms of average year, it is seen that the clusters cover the time period from 2019 to 2021, depending on the average publication year of the data points in each cluster. This indicates that the studies on the recover function involve a mix of relatively recent and somewhat older research points. In general, clusters in the recovery function, "scoping studies", "false data injection attacks", "malicious attack resistance", "efficient production", "data decryption", "rail transport industry", "rail communication case studies" covers topics such as "data analysis" and "digital forensics analysis". The clusters show different dimensions, silhouette coefficients, thematic focuses, and how

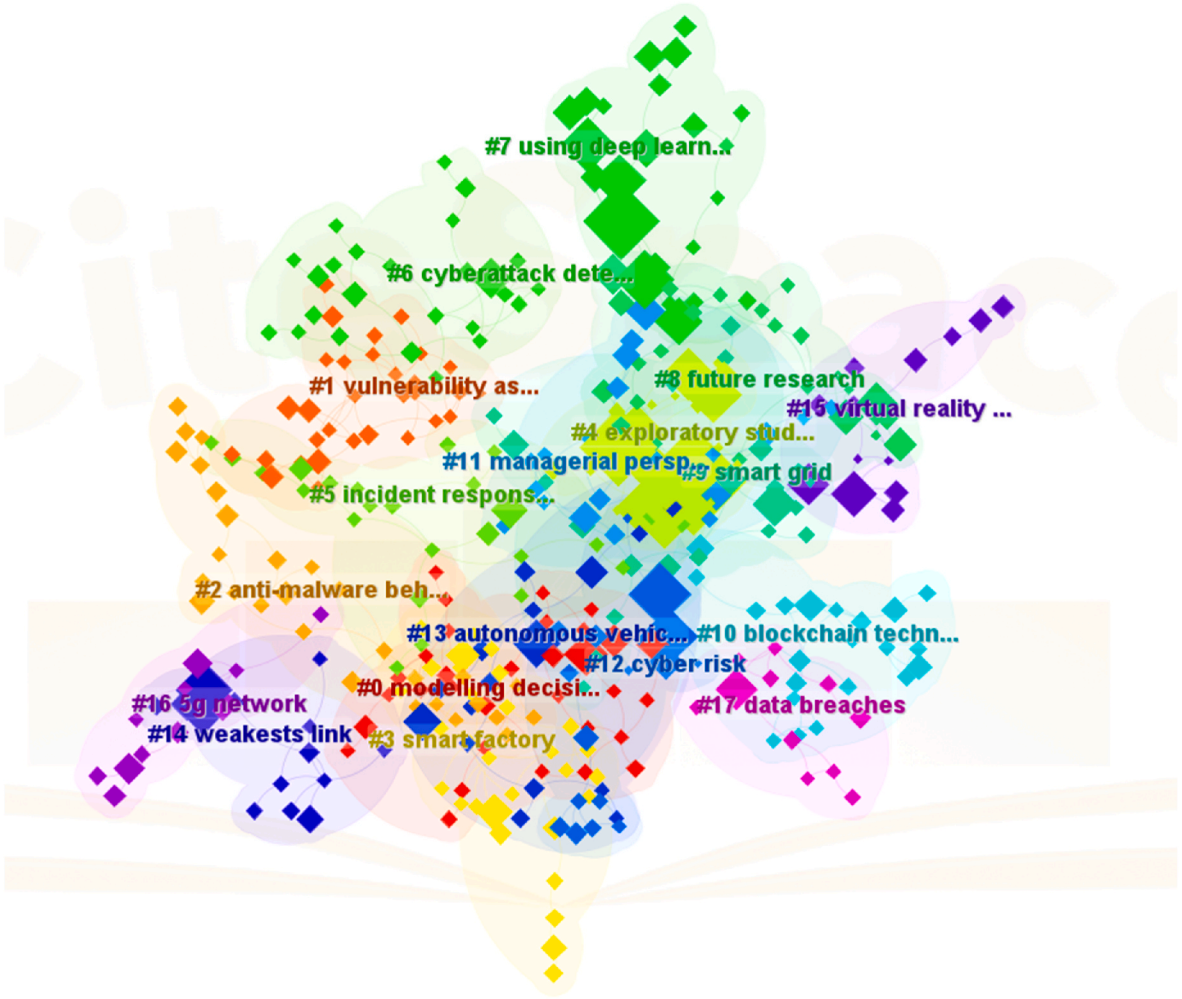


Fig. 3. Cluster analysis (Identify).

well they differentiate from each other, reflecting the diversity and complexity of the recovery function in the context of cybersecurity (Table 5).

When we analyze the scientific research on the rescue function; NIST's cybersecurity framework recovery functions are observed to be spread across multiple clusters. In other words, it can be said that clusters covering different areas that are vital for each cyber resilience and recovery function have emerged. Clusters define specific areas, from combating malicious attacks and mitigating DoS attacks to protect critical infrastructure such as the rail transport industry and programmable logic controllers. There are also quests for the necessity of efficiently securing production processes and decrypting data after cyber incidents. On the other hand, efforts to develop methodologies for digital forensic analysis, which investigate case studies in railway communications and are necessary for post-event investigations, also attract attention. These clusters also provide important clues as they reflect NIST's holistic approach to cyber security, addressing various threats and sectors and ensuring resilience and continuity in the face of evolving cyber risks (Fig. 7).

2.1.6. Comparing all components of NIST cybersecurity framework in terms of social network analysis metrics

2.1.6.1. Keywords. To examine the functions defined in the NIST Cybersecurity framework, which is the cyber security framework standard, we have considered metrics based on social network analysis. In this context, we especially evaluated these functions defined as identify, protect, detect, respond, and recover. We looked at the necessary indicators to determine the roles of the keywords under these functions with their social network analysis values. We started to work by identifying the degree of connectivity, the indicator of centrality betweenness, the identification of nodes with high constraints, and the identification of nodes with low constraints. In the next step, we continued the analysis by listing the top 25 keywords of the rankings formed by the nodes under each function. In this way, it gave the opportunity to make inferences about the determination of the nodal points that continue to be important in the functions determined in the context of the cyber security framework according to the NIST standard, the detection of the nodes that will lose their importance, and the determination of the sub-technology areas that can be defined as open to development or relatively untouched areas. In this part of the study, a comparison process based on social network analysis values was made. According to this comparison, the roles and scores of the keywords in the cyber security framework function list defined by NIST are compared according to their social network analysis values.

When we analyze them according to their functions, the terms "Security," "Computer Security," and "Information Security" among the headings under the Identify heading are closely related to the Identify function. These topics are about identifying and analyzing vulnerabilities, threats or vulnerabilities. In addition, "Privacy" and "Blockchain" headers can also be linked to identification, data privacy and security can be said to be a part of this function. The titles "Cybersecurity," "Machine Learning," and "Internet of Things" under Protect can be associated with the Protect function. These topics include implementing

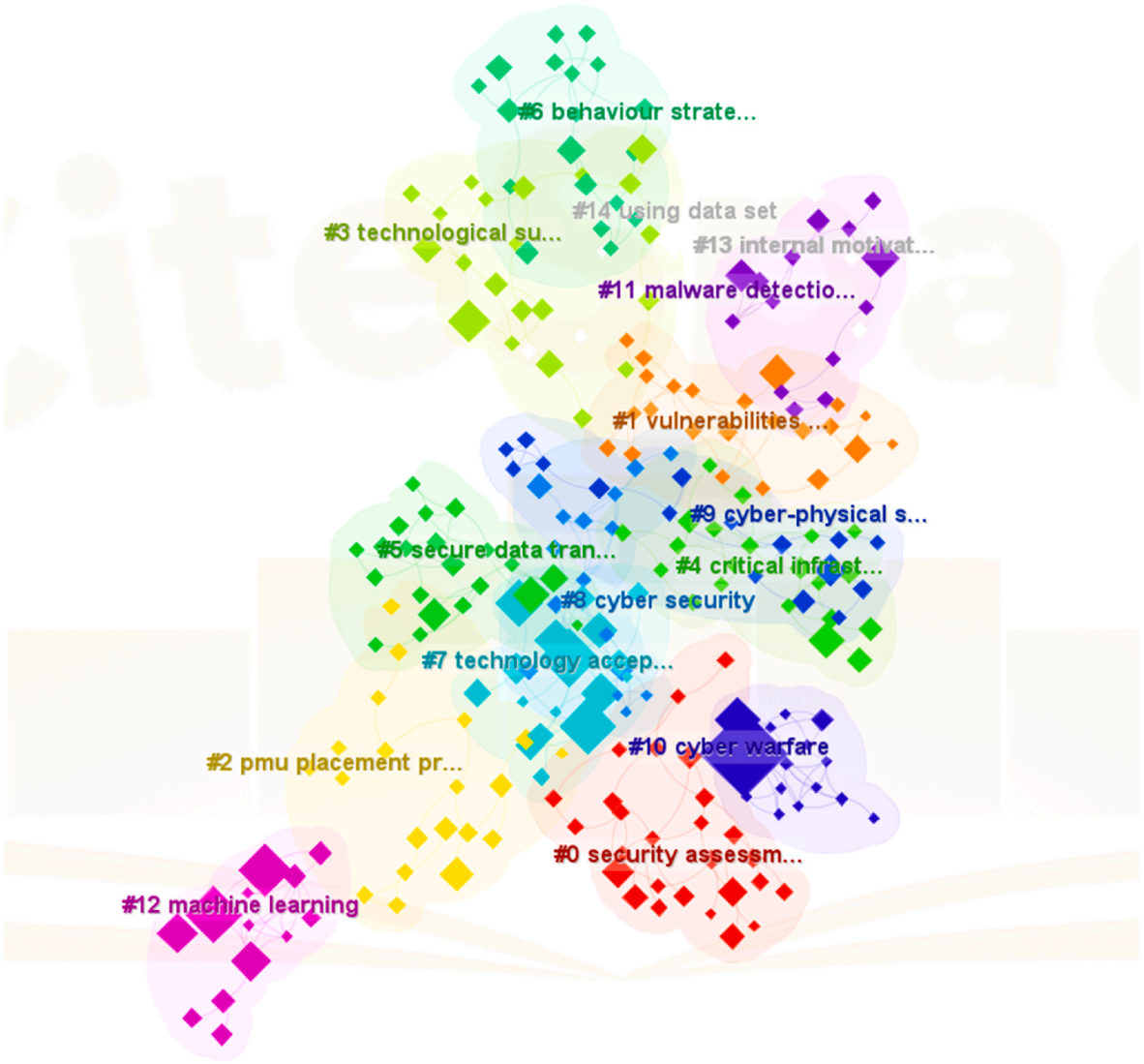


Fig. 4. Cluster analysis (Protect).

security measures, protecting against attacks, and securing systems. In addition, the title "Computer Crime" can also be linked to the protection function, taking measures against criminal activities is part of this function. As for the Detect function, the titles "Cybersecurity," "Machine Learning," and "Deep Learning" are closely related to the Detect function. These topics are directly related to detecting anomalies, attacks or harmful activities and using early warning systems. "Intrusion Detection" and "Anomaly Detection" headings can also be shown as other topics to be associated with this function. In the Respond function, the concepts of "Cybersecurity," "Machine Learning," and "Security" stand out as components that include reacting, responding, and taking necessary measures to attacks or anomalies quickly and effectively. "Phishing" and "Covid-19" headings stand out as headings that can be associated with the Respond function and draw attention to the importance of responding to attacks or emergencies. Finally, in the Recover function, the "Cybersecurity," "Machine Learning," and "Computer Security" titles stand out as the titles associated with the Recover function, which include the subjects of restoring, repairing, and improving systems after attacks. "Smart Grid" and "Critical Infrastructure" headings stand out as structures that need to be rapidly improved after attacks, especially energy systems or critical infrastructures, which can be associated with the Recover function (Table 6).

If it is necessary to analyze and compare the similarities and differences between the concepts gathered under five functions, the concepts gathered under the Identify function include "Security", "Machine Learning", "Internet of Things", "Computer Security", "Deep Learning", "Computer Crime", " It seems that there are terms such as "Anomaly Detection". While these concepts are generally concerned with the identification, analysis and classification of security threats and vulnerabilities, terms such as "Cybersecurity" and "Privacy" stand out among the terms with high centralization value. It can be said that these concepts focus on determining security and privacy issues. Among the concepts gathered under the Protect function are terms such as "Cybersecurity", "Security", "Machine Learning", "Internet of Things", "Computer Security", "Privacy". These concepts deal with the implementation of security measures, the protection of systems, and the prevention of vulnerabilities. While the terms "Cybersecurity" and "Security" stand out among the terms with high centralization value, it is possible to say that these terms represent general security measures and protection strategies. The concepts gathered under the Detect function are "Cybersecurity", "Machine Learning", "Deep Learning", "Internet of Things", "Computer Security", "Anomaly Detection". These concepts prioritize the detection of security breaches and attacks, the detection of anomalies, and the analysis of events. While "Cybersecurity" and "Machine Learning" stand out among terms with high centralization value. These terms appear to represent important tools and techniques for the

Table 2
Summary of the largest 15 clusters (Protect).

Cluster ID	Size	Silhouette	Label (LLR)	Average Year
0	27	0.834	security assessment methodologies (85.3, 1.0E-4)	2016
1	23	0.809	vulnerabilities risks nist perspective (90.47, 1.0E-4)	2019
2	21	0.773	pmu placement protection (57.71, 1.0E-4)	2018
3	21	0.905	technological survey (104.29, 1.0E-4)	2016
4	21	0.791	critical infrastructure (106.11, 1.0E-4)	2016
5	21	0.817	secure data transmission (91.4, 1.0E-4)	2017
6	20	0.923	behaviour strategies (102.18, 1.0E-4)	2018
7	17	0.946	technology acceptance (72.91, 1.0E-4)	2015
8	17	0.96	cyber security (71.21, 1.0E-4)	2016
9	16	0.891	cyber-physical security (91, 1.0E-4)	2018
10	15	1	cyber warfare (138.87, 1.0E-4)	2015
11	14	0.899	malware detection (115.57, 1.0E-4)	2019
12	14	1	machine learning (141.78, 1.0E-4)	2019
13	8	1	internal motivator (79.03, 1.0E-4)	2018
14	7	0.978	using data set (77.45, 1.0E-4)	2013

detection and analysis of security incidents. Under the Respond function, there are terms such as "Cyberattack", "Covid-19", "Threat Analysis", "Response", "Game Theory", "Risk Management". It can be said that these concepts are related to responding to security events and threats, stopping attacks and crisis management. Among the terms with high centralization value, "Cyberattack" and "Covid-19" stand out. These terms represent strategies for responding to cyber-attacks and outbreaks. Finally, it has been observed that there are terms such as "Smart Grid", "Covid-19", "Critical Infrastructure", "Response", "Game Theory", "Risk Management" in the Recover function. These concepts are directly related to the recovery, restructuring and normal functioning of systems after attacks and incidents. Among the terms with high centralization value, "Smart Grid" and "Covid-19" stand out. It can be said that these terms represent terms for the recovery of energy grids and post-pandemic recovery strategies (Table 7).

Among the concepts gathered under the identify function are terms such as "Security", "Machine Learning", "Internet of Things", "Computer Crime", "Computer Security", "Deep Learning". These terms relate to identification processes such as identifying security threats, data analysis, and threat classification. It is observed that "Security" and "Computer Security" stand out among the terms with high centralization value representing general security issues and the security of computer systems. Among the concepts gathered under the Protect function are terms such as "Cybersecurity", "Security", "Feature Extraction", "Machine Learning", "Security of Data", "Computer Security". These terms relate to systems protection, enforcement of security measures, data security and access controls. Among the terms with high centralization value, "Cybersecurity" and "Security" stand out. These terms represent general

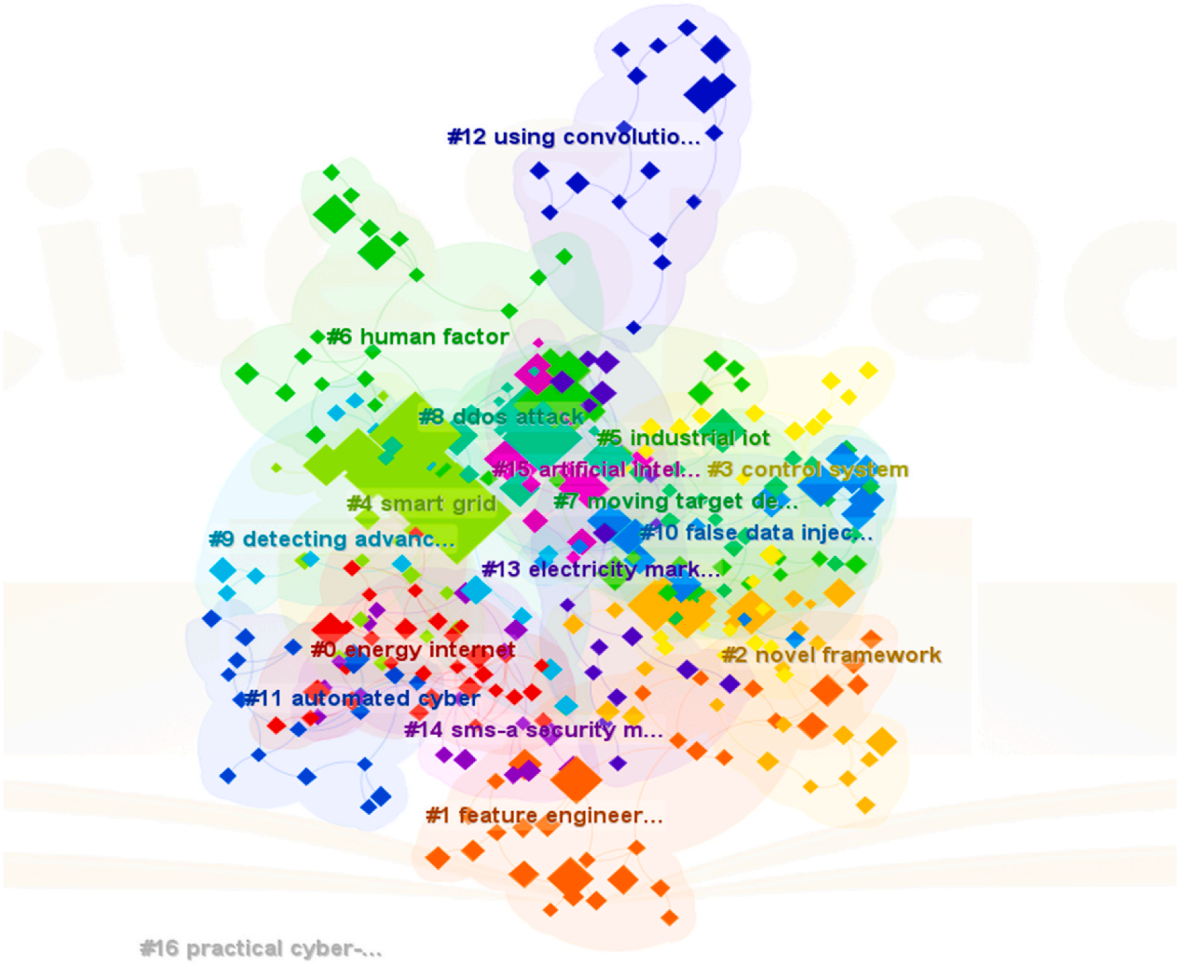


Fig. 5. Cluster analysis (Detect).

Table 3
Summary of the largest 17 clusters (Detect).

ClusterID	Size	Silhouette	Label (LLR)	Average Year
0	32	0.867	energy internet (140.76, 1.0E-4)	2017
1	31	0.919	feature engineering (210.79, 1.0E-4)	2018
2	28	0.954	novel framework (315.07, 1.0E-4)	2018
3	25	0.929	control system (183.84, 1.0E-4)	2018
4	25	0.942	smart grid (327.38, 1.0E-4)	2017
5	25	0.914	industrial IoT (279.4, 1.0E-4)	2018
6	21	0.9	human factor (151.14, 1.0E-4)	2018
7	21	0.909	moving target defense approach (180.22, 1.0E-4)	2018
8	20	0.976	ddos attack (308.44, 1.0E-4)	2011
9	19	0.99	detecting advanced persistent threat (242.05, 1.0E-4)	2018
10	18	0.893	false data injection attack (399.57, 1.0E-4)	2016
11	18	1	automated cyber (150.48, 1.0E-4)	2018
12	18	0.908	using convolutional neural network (173.15, 1.0E-4)	2018
13	18	0.952	electricity market operation (141.77, 1.0E-4)	2018
14	17	0.909	sms-a security management system (164.41, 1.0E-4)	2016
15	12	0.884	artificial intelligence (169.91, 1.0E-4)	2018
16	6	1	practical cyber-attack detection (119.11, 1.0E-4)	2019

security measures and protection strategies. Concepts gathered under the Detect function consist of terms such as "Cybersecurity", "Cyber-attack", "Machine Learning", "Deep Learning", "Intrusion Detection", "Data Models". These terms relate to detecting security breaches, identifying anomalies, detecting cyber-attacks, and analyzing events. Among the terms with high centralization value, "Cybersecurity" and "Intrusion Detection" stand out. These terms represent important tools and techniques for the detection and analysis of security events. The concepts gathered under the Respond function are.

It creates terms like "Security", "Security of Data", "Cloud Computing", "Phishing", "Threat Analysis", "Anomaly Detection". These terms relate to responding to security incidents, stopping attacks, crisis management, and threat analysis. Among the terms with high centralization value, "Security" and "Anomaly Detection" stand out. These terms represent strategies for reacting to security events and detecting anomalies. Among the concepts gathered under the recovery function There are terms such as "Cybersecurity", "Covid-19", "Smart Grid", "Computer Crime", "Covid-19", "Critical Infrastructure". These terms deal

Table 4
Summary of the largest 10 clusters (Respond).

ClusterID	Size	Silhouette	Label (LLR)	Average Year
0	18	0.901	construction industry (27.75, 1.0E-4)	2016
1	14	0.877	taxonomising countermeasure (37.57, 1.0E-4)	2018
2	14	0.877	cyber conflict (38.57, 1.0E-4)	2019
3	12	0.957	domain-oriented topic discovery (25.13, 1.0E-4)	2018
4	12	0.796	reinforcement learning (22.78, 1.0E-4)	2018
5	11	0.934	open science grid (38.77, 1.0E-4)	2015
6	11	0.89	understanding cybersecurity economics (33.1, 1.0E-4)	2019
7	11	0.98	zero-trust model (33.53, 1.0E-4)	2020
8	10	0.89	zero-day attacks detection (25.66, 1.0E-4)	2018
9	10	0.886	circular economy (24.31, 1.0E-4)	2017

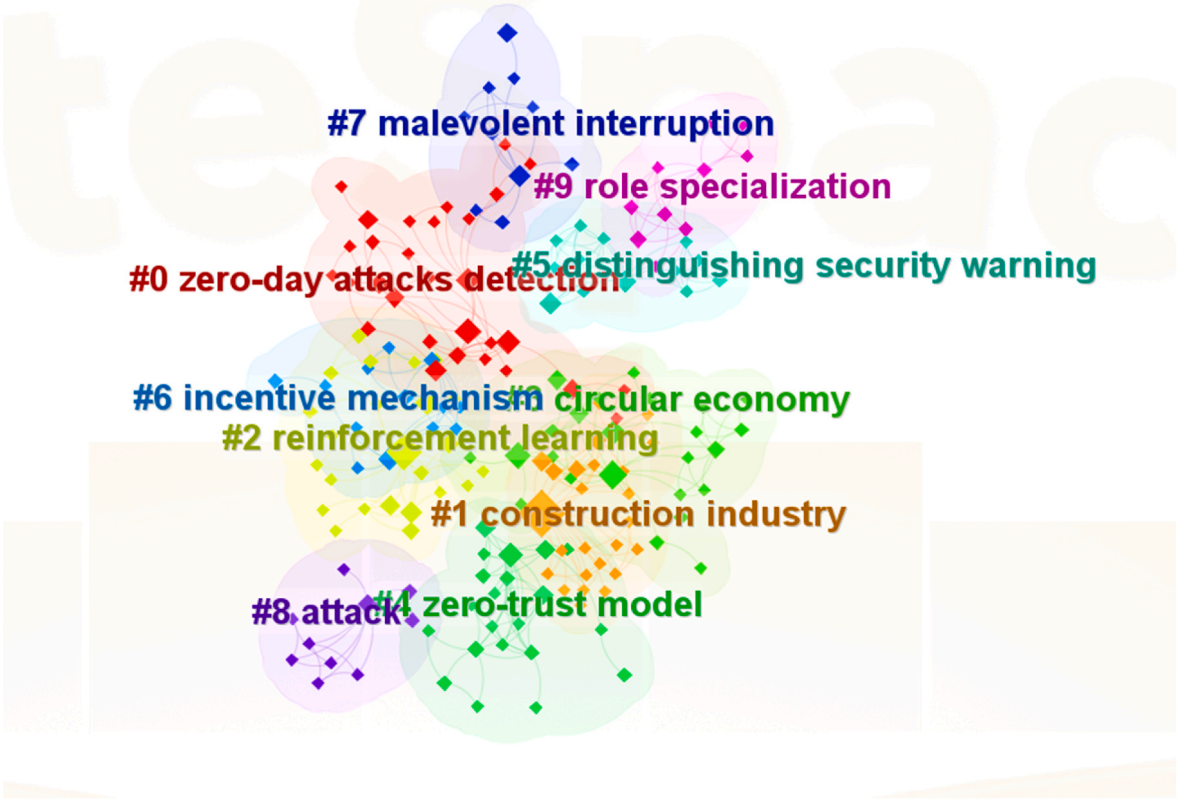


Fig. 6. Cluster analysis (Respond).

Table 5
Summary of the largest 9 clusters (Recover).

Cluster ID	Size	Silhouette	Label (LLR)	Average Year
0	10	1	scoping review (12.54, 0.001)	2021
1	9	0.856	false data injection attack (16.82, 1.0E-4)	2019
2	9	0.929	malicious attack-resilience (13.11, 0.001)	2019
3	8	0.875	efficient manufacturing (15.13, 0.001)	2019
4	8	0.888	decrypting data (14.49, 0.001)	2020
5	8	1	rail transportation industry (14.99, 0.001)	2021
6	5	0.964	railway communication case study (11.46, 0.001)	2019
8	4	0.965	data (4.66, 0.05)	2020
9	3	1	digital forensic analysis (11.99, 0.001)	2021

with the recovery, reconstruction, and normal functioning of systems after attacks and incidents. Among the terms with high centralization value, "Smart Grid" and "Covid-19" stand out. These terms represent strategies for recovering energy grids and post-pandemic recovery. It is worth noting that these concepts are concepts that have reached the level of maturity under each function with high scarcity rates (Table 8).

Low-restriction concepts collected for the identify function include terms such as "Digital Forensics", "Web Security", "Culture", "Connected and Autonomous Vehicles", "Attribution", "Machine Learning (ML)". These terms relate to incident detection, threat detection, digital monitoring, and analysis processes. Among the terms with low centralization value, "Digital Forensics" and "Web Security" stand out. These terms represent digital evidence gathering and web security issues. Concepts with a low restriction rate among those gathered under the Protect function consist of terms such as "Proactive Defense", "Privacy Violation Risk", "Privacy Impact Assessment", "Privacy-Preserving Aggregation", and "Privacy-Preserving Consensus". These terms relate to the implementation of security measures, assessment of privacy risks, data protection and privacy. Among the terms with low centralization value, "Proactive Defense" and "Privacy Violation Risk" stand out. These terms represent active defense strategies and risks associated with privacy breaches. There are terms such as "Cybersecurity Testing", "Human-Machine Interface", "Information Sharing", "Statistical Anomaly Detection", "Cyber Attacks Detection" among the concepts with low restriction rate gathered under Detect. These terms relate to the detection of attacks, detection of anomalies, security testing and information sharing. Among the terms with low centralization value, "Cybersecurity Testing" and "Human-Machine Interface" stand out. These terms represent issues of security testing and human-machine interaction or interface. Concepts with low restrictions in the response function include terms such as "Online Voting", "Municipalities", "Network Flow Forensics", "Malware Traffic Analysis", "Security Operations Center". These terms relate to responding to security incidents, analyzing incidents, monitoring and managing threats. Among the terms with low centralization value, "Online Voting" and "Municipalities" stand out. These terms represent strategies for online voting and the safety of local governments. Concepts with low restriction rate gathered under the Recover function consist of terms such as "Online Voting", "Municipalities", "Network Flow Forensics", "Malware Traffic Analysis", "Security Operations Center". These terms deal with the recovery, reconstruction, and normal functioning of systems after attacks and incidents. Among the terms with low centralization value, "Network Flow Forensics" and "Malware Traffic Analysis" are prominent concepts that usually represent network traffic analysis and malware detection (Table 9).

2.1.6.2. Institutions. Institutions gathered under the identify function include institutions such as "King Saud Univ", "Prince Sattam Bin Abdulaziz Univ", "Chinese Acad Sci", "Univ Texas San Antonio", "Taif Univ". Among the institutions with high centralization value, "King Saud Univ" and "Prince Sattam Bin Abdulaziz Univ" stand out. These institutions can be specified as universities that have important studies on the determination process and information gathering. For the protect function, it is observed that institutions such as "King Saud Univ", "Menoufia Univ", "Umm Al Qura Univ", "Prince Sattam Bin Abdulaziz Univ", "King Abdulaziz Univ" stand out, while "King Saud Univ" and "Prince Sattam" It can be said that institutions such as "Bin Abdulaziz Univ" are among the institutions with high centralization value. It is observed that these institutions are also universities that have

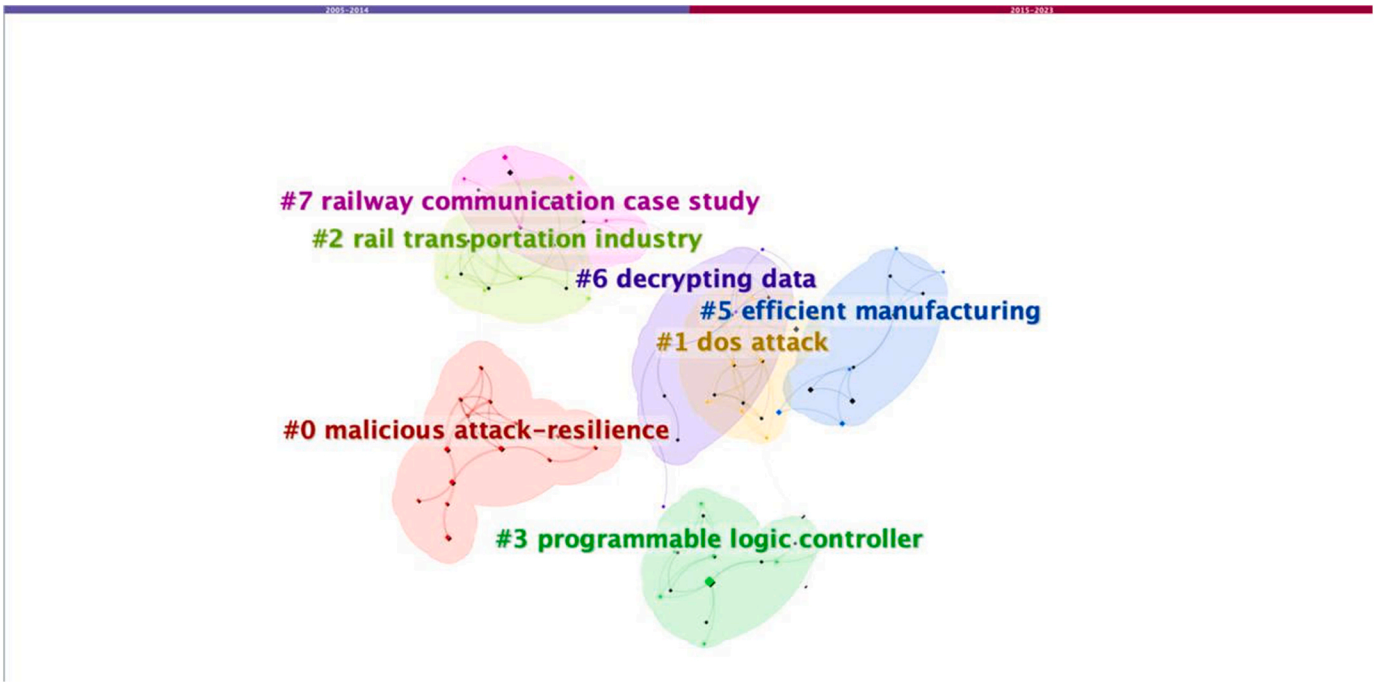


Fig. 7. Cluster analysis (Recover).

Table 6
All degree.

Identify	Protect	Detect	Respond	Recover
Security	Cybersecurity	Cybersecurity	Cybersecurity	Cybersecurity
Machine Learning	Security	Machine Learning	Machine Learning	Security
Internet of Things	Machine Learning	Deep Learning	Security	Machine Learning
Computer Security	Internet of Things	Intrusion Detection	Cyberattack	Computer Security
Deep Learning	Computer Security	Anomaly Detection	Phishing	Covid-19
Computer Crime	Privacy	Security	Computer Security	Smart Grid
Anomaly Detection	Deep Learning	Internet of Things	Smart Grid	Computer Crime
Artificial Intelligence	Intrusion Detection	Feature Extraction	Information Security	Cloud Computing
Intrusion Detection	Computer Crime	Malware	Feature Extraction	Phishing
Privacy	Blockchain	Cyberattack	Covid-19	Threat Analysis
Malware	Smart Grid	Computer Security	Anomaly Detection	Deep Learning
Protocols	Cyber-Security	Computer Crime	Deep Learning	Internet
Cloud Computing	Artificial Intelligence	Artificial Intelligence	Internet of Things	Feature Extraction
Feature Extraction	Malware	Data Models	Cloud Computing	Data Models
Smart Grid	Cyberattack	Cyber-Security	Computer Crime	Critical Infrastructure
Standards	Internet of Things (IoT)	Intrusion Detection System	Internet	Lawsuit
Information Security	Intrusion Detection System	State Estimation	Artificial Intelligence	Target
Blockchain	Cyber-Physical Systems	Support Vector Machines	Critical Infrastructure	Governance
Data Models	Critical Infrastructure	Smart Grid	Privacy	Anomaly Detection
Risk Management	Anomaly Detection	Protocols	Malware	Biological System Modeling
Taxonomy	Information Security	Neural Networks	Cybercrime	Privacy
Support Vector Machines	Authentication	Critical Infrastructure	Complex Systems	Data Breach
Real-Time Systems	Cryptography	Training	Data Models	Internet of Things
Safety	Network Security	Network Security	Data Mining	Decision Making
Computer Architecture	Feature Extraction	Botnet	Decision Making	Malware

Table 7
Betweenness centrality.

Identfy	Protect	Detect	Respond	Recover
Security	Cybersecurity	Cybersecurity	Cybersecurity	Cybersecurity
Machine Learning	Security	Security	Security	Security
Internet of Things	Machine Learning	Machine Learning	Machine Learning	Machine Learning
Computer Security	Internet of Things	Internet of Things	Smart Grid	Smart Grid
Deep Learning	Computer Security	Computer Security	Covid-19	Covid-19
Information Security	Cyber-Security	Cyber-Security	Internet of Things	Internet of Things
Privacy	Privacy	Privacy	Information Security	Information Security
Smart Grid	Smart Grid	Smart Grid	Deep Learning	Deep Learning
Computer Crime	Intrusion Detection	Intrusion Detection	Cybercrime	Cybercrime
Artificial Intelligence	Deep Learning	Deep Learning	Threat Analysis	Threat Analysis
Anomaly Detection	Blockchain	Blockchain	Serious Games	Serious Games
Blockchain	Information Security	Information Security	Response	Response
Malware	Anomaly Detection	Anomaly Detection	Game Theory	Game Theory
Network Security	Artificial Intelligence	Artificial Intelligence	Risk Management	Risk Management
Standards	Network Security	Network Security	Artificial Intelligence	Artificial Intelligence
Intrusion Detection	Computer Crime	Computer Crime	Technology	Technology
Cloud Computing	Cyberattack	Cyberattack	Anomaly Detection	Anomaly Detection
Phishing	Malware	Malware	Cyberattack	Cyberattack
Risk Management	Scada	Scada	Complex Systems	Complex Systems
Human Factors	Cyber-Physical Systems	Cyber-Physical Systems	Surveillance	Surveillance
Risk Assessment	Critical Infrastructure	Critical Infrastructure	Human-Machine Interface	Human-Machine Interface
Covid-19	Authentication	Authentication	Cyber-Attack	Cyber-Attack
Protocols	Internet of Things (IoT)	Internet of Things (IoT)	Threat Hunting	Threat Hunting
Internet	Election Law	Election Law	Internet	Internet
Critical Infrastructure	Cryptography	Cryptography	Computer Security	Computer Security

pioneering studies on protection measures and security policies. In the detect function, it is seen that institutions such as "Prince Sattam Bin Abdulaziz Univ", "Taif Univ", "King Abdulaziz Univ", "Prince Sultan Univ", "Univ Waterloo" are collected, while "Prince Sattam Bin Abdulaziz Univ" is among the institutions with high centralization value. and "Taif Univ". These institutions are universities that stand out with their publications in the field of detection of threats, detection of anomalies and security analysis. It is seen that institutions such as "Univ Illinois", "Tokyo Inst Technol", "Umbc", "City Univ London", "Univ Milan" are gathered under the Respond function. It can be said that "Univ Illinois" and "Tokyo Inst Technol" stand out among the institutions with high centralization value, and these institutions are pioneers with their publications on responding to security incidents, incident analysis and management. In the recovery function, it is possible to see institutions such as "Univ Texas San Antonio", "Fordham Univ", "Nist", "Univ Southampton", "Natl Inst Informat". "Univ Texas San Antonio" and "Nist", which have high centralization values, stand out as institutions that come to the fore in post-attack system recovery, restructuring and continuity (Table 10). When we evaluate the prominent institutions based on functions according to geographical regions, "Univ Texas San Antonio" and "Fordham Univ" in North America are the prominent institutions in post-attack system recovery, restructuring and continuity. "Univ Illinois" is a prominent organization with publications on security incident response, incident analysis and management. In Europe, "Univ Southampton" and "Natl Inst Informat" are institutions that play an important role in post-attack system recovery, restructuring and continuity. "City Univ London" and "Univ Milan" are prominent institutions in security incident response, incident analysis and management. Looking

Table 8
High aggregate constraints (HAC).

Identfy	Protect	Detect	Respond	Recover
Security	Cybersecurity	Cybersecurity	Cybersecurity	Cybersecurity
Machine Learning	Security	Cyberattack	Security	Security
Internet of Things	Computer Security	Feature Extraction	Machine Learning	Machine Learning
Computer Crime	Machine Learning	Machine Learning	Computer Security	Computer Security
Computer Security	Internet of Things	Security	Covid-19	Covid-19
Deep Learning	Organizations	Computer Crime	Smart Grid	Smart Grid
Servers	Data Models	Deep Learning	Computer Crime	Computer Crime
Resilience	Intrusion Detection	State Estimation	Cloud Computing	Cloud Computing
Privacy	Medical Services	Data Models	Phishing	Phishing
Data Models	Computer Crime	Support Vector Machines	Threat Analysis	Threat Analysis
Cloud Computing	Power System Security	Intrusion Detection	Deep Learning	Deep Learning
Automation	Privacy	Computer Security	Internet	Internet
Training	Critical Infrastructure	Computational Modeling	Feature Extraction	Feature Extraction
Critical Infrastructure	Smart Grids	Training	Data Models	Data Models
Computer Architecture	Informatics	Internet of Things	Critical Infrastructure	Critical Infrastructure
Data Mining	Computer Hacking	Power Systems	Lawsuit	Lawsuit
Risk Management	Security Of Data	Power System Dynamics	Target	Target
Survey	Cyber-Physical Systems	Phasor Measurement Units	Governance	Governance
Licenses	Protocols	False Data Injection Attack	Anomaly Detection	Anomaly Detection
Integrated Circuits	Security And Privacy	Protocols	Biological System Modeling	Biological System Modeling
Protocols	Network Intrusion Detection	Servers	Privacy	Privacy
Big Data	Real-Time Systems	Ip Networks	Data Breach	Data Breach
Information Security	Deep Learning	IoT	Internet of Things	Internet of Things
Computer Hacking	Correlation	Performance Evaluation	Decision Making	Decision Making
Networks	Power Grids	Malware	Malware	Malware

Table 9
Low aggregate constraints (LAC).

Identify	Protect	Detect	Respond	Recover
Digital Forensics	Proactive Defense	Cybersecurity Testing	Online Voting	Online Voting
Web Security	Privacy Violation Risk	Human-Machine Interface	Municipalities	Municipalities
Culture	Privacy Impact Assessment	Information Sharing	Network Flow Forensics	Network Flow Forensics
Connected And Autonomous Vehicles	Privacy-Preserving Aggregation	Statistical Anomaly Detection	Malware Traffic Analysis	Malware Traffic Analysis
Attribution	Privacy-Preserving Consensus	Cyber Attacks Detection	Security Operations Center	Security Operations Center
Machine Learning (Ml)	Security Standards	Application Layer	Neurosecurity	Neurosecurity
Information Security Management	User Awareness	Web Application Security	User Interface Design	User Interface Design
International Law	Countermeasure	Energy Management System	Security Warning	Security Warning
Due Diligence	Electronic Voting	Security Policies	Voting Standards	Voting Standards
Power System State Estimation	Attack Graph	Pattern Mining	Security Analysis and Valuation	Security Analysis and Valuation
Bioeconomy	Human Factors	Web Vulnerabilities	Security Information and Event Management (Siem) Systems	Security Information and Event Management (Siem) Systems
Hardware Trojan	Self-Efficacy	Return-Oriented Programming	Resilient Event Storage	Resilient Event Storage
Human Rights	Transportation Security	Fuzzing	Security Protocols	Security Protocols
Socio-Technical Systems	Simulation	Developing Countries	Risk Scoring	Risk Scoring
Synchrophasors	Higher Education Institution	Program Slice	Reputation Propagation	Reputation Propagation
Cross-Border Health Data Exchange	Data Sharing	Data Quality	Renewable Mitigation	Renewable Mitigation
Interviews	Proactive Secure Scheme	Cyber Attack Detection	Regional Cooperation	Regional Cooperation
Medical Device	Fintech	Drdos	Peace-Making	Peace-Making
Social Networks	Model	Design Science	Thompson Sampling	Thompson Sampling
Information Assurance	Moving Target Defense (Mtd)	Complex Event Processing	Paillier Cryptosystem	Paillier Cryptosystem
Useable Security	Eu Law	Cybersecurity Of Substations	Smart Home (Sh)	Smart Home (Sh)
Blockchain Technology	Spear Phishing	Bots	Pending Intent	Pending Intent
Information Warfare	Cardiovascular Implantable Electronic Devices	Automatic Generation Control	Mahalanobis Distance Metric	Mahalanobis Distance Metric
Geopolitics	Decision Support System	Malicious Url	Warnings	Warnings
Threat Modelling	Architectural Tactic	Safety	Zero-Days Attack	Zero-Days Attack

at the Middle East.

"King Saud Univ", "Prince Sattam Bin Abdulaziz Univ", "Umm Al Qura Univ" and "King Abdulaziz Univ" appear to be prominent institutions in the protection function, while "Prince Sattam Bin Abdulaziz Univ", "Taif Univ" and "King Abdulaziz Univ" Abdulaziz Univ" are leading universities in threat detection, detection of anomalies and security analysis. In Asia, "Chinese Acad Sci" excels in threat detection, detection of anomalies and security analysis. "Tokyo Inst Technol" is a prominent

Table 10
Degree.

Identify	Protect	Detect	Respond	Recover
King Saud Univ	King Saud Univ	Prince Sattam Bin Abdulaziz Univ	Univ Illinois	Tokyo Inst Technol
Prince Sattam Bin Abdulaziz Univ	Menoufia Univ	Taif Univ	Umbc	Nanyang Technol Univ
Chinese Acad Sci	Umm Al Qura Univ	King Abdulaziz Univ	Taif Univ	Univ Macau
Univ Texas San Antonio	Univ Jeddah	Prince Sultan Univ	City Univ London	Zhejiang Gongshang Univ
Taif Univ	Taif Univ	Umm Al Qura Univ	Univ Milan	Fordham Univ
Charles Darwin Univ	King Abdulaziz Univ	Princess Nourah Bint Abdulrahman Univ	Sphynx Technol Solut Ag	Cent South Univ
Univ Waterloo	Princess Nourah Bint Abdulrahman Univ	Swinburne Univ Technol	Simplan	Guangzhou Univ
Air Univ	La Trobe Univ	Deakin Univ	Social Engn Acad	Huaqiao Univ
Deakin Univ	Prince Sattam Bin Abdulaziz Univ	Univ Waterloo	Tuv Hellas Tuv Nord Sa	East China Univ Sci & Technol
Univ Oxford	Minia Univ	Asia Univ	Itml	Carnegie Mellon Univ
George Mason Univ	Edith Cowan Univ	Chinese Acad Sci	Atos Spain Sa	Nyu
Purdue Univ	Macquarie Univ	Univ Texas San Antonio	Danaos Shipping Co	Univ Southampton
Nanyang Technol Univ	Sphynx Technol Solut Ag	Virginia Tech	Tech Univ Crete	Fdn Univ Ceipa
Georgia Inst Technol	Imam Abdulrahman Bin Faisal Univ	King Saud Univ	Fdn Res & Technol Hellas	Cotecmar
King Abdulaziz Univ	Fdn Res & Technol Hellas	King Khalid Univ	Hellen Mediterranean Univ Hmu	Nist
Prince Sultan Univ	Tech Univ Crete	Manchester Metropolitan Univ	Sungkyunkwan Univ	Shenzhen Inst Artificial Intelligence & Robot Soc
Univ Warwick	Kyungpook Natl Univ	Vellore Inst Technol	Cyber Def Lab	Univ Sydney
Univ Piraeus	Swinburne Univ Technol	Univ Management & Technol	Dept Curriculum & Instruct	Swinburne Univ Technol
Univ Maryland	Univ Milan	Menoufia Univ	Illinois Foundry Innovat Engn Educ	Xidian Univ
Umm Al Qura Univ	Kafrelsheikh Univ	Lebanese Amer Univ	Secondary Educ Dept	Shibaura Inst Technol
Princess Nourah Bint Abdulrahman Univ	Univ Nebraska	Natl Taiwan Univ Sci & Technol	Univ Texas San Antonio	Csiro
Indiana Univ	Univ Waterloo	Univ New South Wales	Univ Houston	Natl Inst Informat
Univ Padua	Norwegian Univ Sci & Technol	Qatar Univ	Vignana Bharathi Inst Technol	Ut Mem Hermann Ctr Hlth Care Qual & Safety
Vellore Inst Technol	Lulea Univ Technol	Macquarie Univ	Anal Comp & Engn Solut	Baylor Coll Med
Univ Technol Sydney	Virginia Tech	Air Univ	Queensland Univ Technol	Michael E Debakey Va Med Ctr

Table 11
Betweenness centrality.

Identify	Protect	Detect	Respond	Recover
King Saud Univ	Taif Univ	King Abdulaziz Univ	Univ Oxford	Nanyang Technol Univ
Univ Texas San Antonio	La Trobe Univ	Prince Sattam Bin Abdulaziz Univ	Univ Warwick	Xian Univ Technol
Univ Waterloo	Guangzhou Univ	Chinese Acad Sci	Georgia State Univ	Carnegie Mellon Univ
Univ Oxford	Air Univ	Virginia Tech	City Univ London	Ajou Univ
George Mason Univ	Rmit Univ	Singapore Univ Technol & Design	Alan Turing Inst	Tokyo Inst Technol
Indiana Univ	King Saud Univ	Taif Univ	Taif Univ	Fdn Univ Ceipa
Tsinghua Univ	Swinburne Univ Technol	Swinburne Univ Technol	Sungkyunkwan Univ	Cotecmar
Chinese Acad Sci	Norwegian Univ Sci & Technol	Univ Waterloo	Univ Virginia	Nyu
Deakin Univ	Fordham Univ	Univ Management & Technol	Queensland Univ Technol	Univ Macau
Univ Melbourne	Menoufia Univ	Umm Al Qura Univ	Carnegie Mellon Univ	Zhejiang Gongshang Univ
Univ Warwick	Univ Technol Sydney	Northeastern Univ	Univ Milan	Fordham Univ
King Abdulaziz Univ	Minia Univ	Univ Texas San Antonio	Coventry Univ	Cent South Univ
Air Univ	Deakin Univ	Univ Illinois	Air Univ	Guangzhou Univ
Charles Darwin Univ	Edith Cowan Univ	King Saud Univ	Qatar Univ	Huaqiao Univ
Purdue Univ	Univ Jeddah	Shanghai Jiao Tong Univ	Chinese Acad Sci	East China Univ Sci & Technol
Univ Padua	Univ New South Wales	Deakin Univ	Univ Melbourne	Univ Southampton
Taif Univ	Macquarie Univ	Aalborg Univ	Virginia Polytech Inst & State Univ	Nist
Washington State Univ	Univ Aegean	Aston Univ	Southeast Univ	Shenzhen Inst Artificial Intelligence & Robot Soc
Swinburne Univ Technol	Univ Illinois	Univ Calgary	Univ Tennessee	Univ Sydney
Univ Technol Sydney	Lulea Univ Technol	Southeast Univ	Argonne Natl Lab	Swinburne Univ Technol
Univ Piraeus	King Abdulaziz Univ	Virginia Polytech Inst & State Univ	Univ Illinois	Xidian Univ
Qatar Univ	Qatar Univ	Univ Technol Sydney	Univ Cent Florida	Shibaura Inst Technol
Univ Maryland	Univ Texas San Antonio	Sichuan Univ	Univ Michigan	Csiro
Univ Strathclyde	Michigan Technol Univ	Nanyang Technol Univ	George Mason Univ	Natl Inst Informat
Mississippi State Univ	Vellore Inst Technol	Hong Kong Polytech Univ	Chungnam Natl Univ	Ut Mem Hermann Ctr Hlth Care Qual & Safety

Table 12
High aggregate constraints.

Identify	Protect	Detect	Respond	Recover
Prince Sattam Bin Abdulaziz Univ	Menoufia Univ	King Abdulaziz Univ	City Univ London	Nanyang Technol Univ
King Saud Univ	King Saud Univ	Prince Sattam Bin Abdulaziz Univ	Sphynx Technol Solut Ag	Ajou Univ
Indiana Univ	Deakin Univ	Taif Univ	Simplan	Xian Univ Technol
Univ Texas Dallas	Umm Al Qura Univ	Umm Al Qura Univ	Social Engn Acad	Carnegie Mellon Univ
Northeastern Univ	Birmingham City Univ	Univ New South Wales	Tuv Hellas Tuv Nord Sa	Univ Macau
Northumbria Univ	Prince Sattam Bin Abdulaziz Univ	Vellore Inst Technol	Itml	Zhejiang Gongshang Univ
Macquarie Univ	Univ Technol Sydney	Macquarie Univ	Atos Spain Sa	Fordham Univ
Georgia Inst Technol	Univ Jeddah	Deakin Univ	Danaos Shipping Co	Cent South Univ
Taif Univ	Future Univ Egypt	Jouf Univ	Tech Univ Crete	Guangzhou Univ
Huazhong Univ Sci & Technol	Macquarie Univ	Swinburne Univ Technol	Fdn Res & Technol Hellas	Huaqiao Univ
George Mason Univ	King Abdulaziz Univ	Virginia Tech	Hellen Mediterranean Univ Hmu	Tokyo Inst Technol
Univ Kent	Edith Cowan Univ	Univ Technol Sydney	Univ Oxford	Xi An Jiao Tong Univ
Purdue Univ	Swinburne Univ Technol	Shanghai Jiao Tong Univ	Univ Cent Florida	Shenzhen Inst Artificial Intelligence & Robot Soc
Univ Texas San Antonio	Univ Jordan	Aalborg Univ	Univ Portsmouth	Univ Sydney
Univ New South Wales	Univ Milan	Univ Texas San Antonio	Univ Texas San Antonio	Chinese Univ Hong Kong
Princess Nourah Bint Abdulrahman Univ	Lulea Univ Technol	Nanyang Technol Univ	Univ Illinois	Fdn Univ Ceipa
Univ Wollongong	Univ Sci & Technol Beijing	King Khalid Univ	Taif Univ	Cotecmar
Qatar Univ	Univ Waterloo	King Saud Univ	Carnegie Mellon Univ	Acad Sinica
Chongqing Univ	China Acad Engn Phys	Virginia Polytech Inst & State Univ	Argonne Natl Lab	Natl Taiwan Univ Sci & Technol
Kyung Hee Univ	Univ Texas San Antonio	Singapore Univ Technol & Design	Tech Univ Munich	Inst Informat Ind
Rmit Univ	Virginia Tech	Univ Management & Technol	Umbc	Univ Fed Rio De Janeiro
Delft Univ Technol	Babasaheb Bhimrao Ambedkar Univ	Mit	Georgia State Univ	Univ Cyprus
Air Univ	Minia Univ	Norwegian Univ Sci & Technol	Univ Jyvaskyla	Swinburne Univ Technol
Univ Technol Sydney	Purdue Univ	Silesian Tech Univ	Vignana Bharathi Inst Technol	Xidian Univ
Bahria Univ	Univ Kebangsaan Malaysia	Manchester Metropolitan Univ	Air Univ	Csiro

institution with publications on security incident response, incident analysis and management.

"King Saud Univ", "Univ Texas San Antonio", "Univ Waterloo", "Univ Oxford", "George Mason Univ" come to the fore among the institutions with high betweenness centrality in the identify function. While these institutions stand out as leading universities in the determination process and information gathering, institutions such as "King Saud Univ" and "Univ Oxford" have a particularly strong position in the field of determination. Institutions with high Centralization value in the Protect function include "Taif Univ", "La Trobe Univ", "Guangzhou Univ", "Air Univ", "Deakin Univ". These institutions can be defined as universities that are pioneers in protection measures and security policies. On the other hand, institutions such as "Taif Univ" and "La Trobe Univ" are institutions that have effective studies in the field of conservation. Among the institutions with high Detect Centralization value, "King Abdulaziz Univ", "Prince Sattam Bin Abdulaziz Univ", "Chinese Acad Sci", "Virginia Tech", "Univ Illinois" stand out. These institutions are universities that are pioneers in threat detection, detection of anomalies and security analysis. Institutions such as "King Abdulaziz Univ" and "Chinese Acad Sci" can also be characterized as institutions that have a strong position in detection. Institutions with high Respond Centralization value include "Univ Oxford", "City Univ London", "Alan Turing Inst", "Tokyo Inst Technol", "Ajou Univ". These organizations are pioneers in security incident response, incident analysis and management. Institutions such as "Univ Oxford" and "Tokyo Inst Technol" can be cited among other institutions that have effective work in the field of response. Among the institutions with high Centralization value for the recovery function, "Nanyang Technol Univ", "Xian Univ Technol", "Carnegie Mellon Univ", "Tokyo Inst Technol", "Cent South Univ" stand out. structuring and continuity. Institutions such as "Nanyang Technol Univ" and "Carnegie Mellon Univ" are among other institutions that have a strong position in the rescue field (Table 11).

Institutions with a high aggregate constraints in the identify function include "Prince Sattam Bin Abdulaziz Univ", "King Saud Univ", "Indiana Univ", "Univ Texas Dallas", and "Northeastern Univ". Although these institutions have a high level of connectivity in the determination process, they are still universities that can work effectively. It can be said that institutions such as "King Saud Univ" and "Prince Sattam Bin Abdulaziz Univ" have an important role in the network and are among the important institutions that are effective in determining their place in the network, even if there is a movement constraint in terms of social network dynamics. "Menoufia Univ", "King Saud Univ", "Deakin Univ", "Umm Al Qura Univ", "Birmingham City Univ" stand out among the institutions with a high aggregate constraints in the protect function. These institutions are universities that operate with limited resources in the conservation processes. Institutions such as "Deakin Univ" and "Umm Al Qura Univ" are institutions that have effective studies on protection despite the high aggregate constraint. "King Abdulaziz Univ", "Prince Sattam Bin Abdulaziz Univ", "Taif Univ", "Umm Al Qura Univ", "Vellore Inst Technol" stand out among the institutions with high aggregate constraints. These institutions are active in threat detection and security analysis with limited momility in terms of social network dynamics. Institutions such as "King Abdulaziz Univ" and "Prince Sattam Bin Abdulaziz Univ" are institutions that have effective studies on detection, despite their high aggregate constraint. Institutions with high aggregate constraint on Respond include "City Univ London", "Sphynx Technol Solut Ag", "Simplan", "Social Engn Acad", "Danaos Shipping Co". These institutions are universities that are active in reacting and managing events with limited flexibility in terms of social network dynamics. Institutions such as "City Univ London" and "Danaos Shipping Co" are institutions that have scientific publications on effective response processes, despite the high aggregate constraint. "Nanyang Technol

Table 13
Low Aggregate constraint.

Identify	Protect	Detect	Respond	Recover
Kobe Univ	Sci Inst Publ Law	Univ Patras	Univ Fed Rio De Janeiro	Univ Illinois
Univ Rijeka	St Petersburg State Univ	Univ Politecn Cataluna	Wayne State Univ	Natl Assoc Insurance Commissioners
World Maritime Univ	Waterford Inst Technol	North Carolina A&T State Univ	Serv Madriletio Salud	Telkom Univ
Suny Buffalo	Singapore Univ Technol & Design	Florida Int Univ	Atos Res & Innovat	Police Forens Lab Ctr
Inst Rural Management Anand Irma	Univ Fuerzas Armadas Espe	Univ West Florida	Natl Univ Sci & Technol	Siemens Ag
Dalian Maritime Univ	St Francis Xavier Univ	Florida Polytech Univ	Inst Def Studies & Anal	Friedrich Alexander Univ Erlangen Nuremberg
Univ Bradford	Natl Acad Internal Affairs	Yarmouk Univ	Univ Brasilia Unb	Univ Colorado
Texas A&M Univ	Russian State Univ Humanities	Al Al Bayt Univ	Univ Complutense Madrid Ucm	Univ Chile
Novartis Pharma Ag	Unsw Sydney	Princess Sumaya Univ Technol	Univ Brasilia	Virginia Tech
Philips Engn Solut	Univ Hong Kong	Univ Chinese Acad Sci	Univ Brighton	Univ Chinese Acad Sci
Us Mil Acad	Shamoon Coll Engn	Natl Inst Metrol Qual & Technol	Stockholm Univ	Univ Warwick
Clemson Univ	Syst On Chip Engn	Univ Fed Rio De Janeiro	Univ East London	Natl Chin Yi Univ Technol
Bila Tserkva Natl Agr Univ	Univ Basque Country	Eller Coll Management	Anglia Ruskin Univ	West Pomeranian Univ Technol Szczecin
Natl Acad Internal Affairs	Univ Chinese Acad Sci	Ecole Polytech Fed Lausanne	Univ Essex	Ibm Polska Sp Zoo
Borys Grinchenko Kyiv Univ	Univ Dist Columbia	Univ Calif Davis	T2 Doo	West Pomeranian Univ Technol
Natl Acad Secur Serv Ukraine	Iowa State Univ	State Univ Londrina Uel	Fernuniv	Univ South Australia
Krasnodar Univ	Howard Univ	Univ Cadiz	Sun Moon Univ	Univ Penn
Kazan Innovat Univ	Irt Systemx	Univ Sao Paulo	Kyunggi Univ	Univ Teknol Mara Uitm
Univ Montreal	New Jersey Inst Technol	Univ Informat Technol	Sogang Univ	Univ Melbourne
Ericsson Montreal	Brigham & Womens Hosp	Nanjing Univ Informat Sci & Technol	Univerza Mariboru	Rmit Univ
Naif Arab Univ Secur Sci	Technol Inst Philippines Quezon City	Univ So Calif	Univ Washington	Univ Southern Calif
Korea Univ	Univ Guelph	Yazd Univ	Waterford Inst Technol	Gazi Univ
Peace Res Inst Frankfurt	European Univ	Keene State Coll	Univ Zurich Uzh	Hacettepe Univ
Oregon State Univ	Univ Informat Technol	Fdn Policlin Gemelli	Univ Limerick	Feng Chia Univ
Univ Hail	Univ Modena & Reggio Emilia	Univ Basque Country	Confirm Sfi Ctr Smart Mfg	Areva Gmbh

Univ", "Ajou Univ", "Xian Univ Technol", "Carnegie Mellon Univ", "Fordham Univ" stand out among institutions with high aggreagte constraint. These institutions are active in managing recovery processes and restructuring systems with high aggregate constraint. Institutions such as "Nanyang Technol Univ" and "Carnegie Mellon Univ" are institutions that have effective rescue efforts despite their high aggregate constraint.

"Kobe Univ", "Univ Rijeka", "World Maritime Univ", "Suny Buffalo", "Inst Rural Management Anand Irma" are among the institutions with low restriction rates clustered for the identify function. These institutions are universities that have wide resources and flexibility according to the dynamics of social network analysis in the determination process. Institutions such as "Kobe Univ" and "World Maritime Univ" are institutions that have effective studies in identification despite their low constraint rate. In other words, although they have certain limitations in terms of connectivity in the network, it can be said that these two institutions exhibit a profile that is open to development. In the studies on the protect function, it is observed that "Sci Inst Publ Law", "St Petersburg State Univ", "Waterford Inst Technol", "Singapore Univ Technol & Design", "Univ Fuerzas Armadas Espe" addresses stand out among the institutions with low restrictions. These institutions are universities that have wide resources and flexibility according to social network analysis dynamics in conservation processes. Institutions such as "St Petersburg State Univ" and "Singapore Univ Technol & Design" are institutions that have effective studies on conservation despite their low rate of limitations. In other words, they have a development potential in research on conservation function. Institutions with low disability rates gathered under Detect are seen as "Univ Patras", "Univ Politecn Cataluna", "North Carolina A&T State Univ", "Florida Int Univ", "Univ West Florida". Institutions such as "Univ Patras" and "Florida Int Univ" are institutions that draw attention with their effective work on the detection function despite their low restriction rate. Institutions with low restriction rates on Respond include "Univ Fed Rio De Janeiro", "Wayne State Univ", "Serv Madriletio Salud", "Atos Res & Innovat", "Univ East London". These institutions are universities that are active in reacting and managing events by having wide resources and flexibility according to social network analysis dynamics. Institutions such as "Univ Fed Rio De Janeiro" and "Wayne State Univ" are institutions that have scientific research into effective response processes despite their low constraint rate. "Univ Illinois", "Natl Assoc Insurance Commissioners", "Telkom Univ", "Police Forens Lab Ctr", "Siemens Ag" stand out among the institutions with low restrictions under recovery. These institutions are the universities that are active in managing the recovery processes and restructuring the systems by having wide resources and flexibility according to the dynamics of social network analysis (Table 13).

If we evaluate the results of institutions with high constraint rates in terms of geographical regions according to their NIST Functions: In the Identify Function, it is seen that King Saud University and Prince Sattam Bin Abdulaziz University in the Middle East play an important role in the identification process. These universities are important institutions that are influential in determining their place in the network. In North America, Indiana University, University of Texas Dallas, and Northeastern University are institutions with high connectivity in determining function. In Protect Function King Saud University in Saudi Arabia is a leading university in protection measures and security policies. In Australia, La Trobe University and Deakin University are institutions that have effective studies with limited resources. In Detect Function, King Abdulaziz University and Prince Sattam Bin Abdulaziz University in Saudi Arabia are leading universities in threat detection, anomaly detection and security analysis. In China, the Chinese Academy of Sciences is an institution with a strong position in threat detection. Virginia Tech and University of Illinois in the USA are the leading universities in the field of threat detection and security analysis. As for the Respond Function, the University of Oxford and City University London in the UK are the leading institutions in security incident response, incident analysis and management. In Japan, Tokyo Institute of Technology is an institution known for effective response studies. In the Recovery Function, Nanyang Technological University in Singapore is strongly positioned to manage recovery processes and reengineer systems. In the US, Carnegie Mellon University is another institution that has been

Table 14
Aggregate results for topics.

Identify	Protect	Detect	Respond	Recover
modelling decision-making	security assessment methodologies	energy internet	construction industry	scoping review
vulnerability assessment	vulnerabilities risks nist perspective	feature engineering	taxonomising countermeasure	false data injection attack
anti-malware behaviour	pmu placement protection	novel framework	cyber conflict	malicious attack-resilience
smart factory	technological survey	control system	domain-oriented topic discovery	efficient manufacturing
exploratory study	critical infrastructure	smart grid	reinforcement learning	scoping review

Table 15
Aggregate results for institutes.

Identify	Protect	Detect	Respond	Recover
King Saud Univ	**King Saud Univ**	**Prince Sattam Bin Abdulaziz Univ**	Univ Illinois	Tokyo Inst Technol
Prince Sattam Bin Abdulaziz Univ	Menoufia Univ	**Taif Univ**	Umbc	Nanyang Technol Univ
Chinese Acad Sci	Umm Al Qura Univ	King Abdulaziz Univ	**Taif Univ**	Univ Macau
Univ Texas San Antonio	Univ Jeddah	Prince Sultan Univ	City Univ London	Zhejiang Gongshang Univ
Taif Univ	**Taif Univ**	Umm Al Qura Univ	Univ Milan	Fordham Univ
King Saud Univ	**Taif Univ**	King Abdulaziz Univ	Univ Oxford	Nanyang Technol Univ
Univ Texas San Antonio	La Trobe Univ	**Prince Sattam Bin Abdulaziz Univ**	Univ Warwick	Xian Univ Technol
Univ Waterloo	Guangzhou Univ	Chinese Acad Sci	Georgia State Univ	Carnegie Mellon Univ
Univ Oxford	Air Univ	Virginia Tech	City Univ London	Ajou Univ
George Mason Univ	Rmit Univ	Singapore Univ Technol & Design	Alan Turing Inst	Tokyo Inst Technol
Prince Sattam Bin Abdulaziz Univ	Menoufia Univ	King Abdulaziz Univ	City Univ London	Nanyang Technol Univ
King Saud Univ	**King Saud Univ**	**Prince Sattam Bin Abdulaziz Univ**	Sphynx Technol Solut Ag	Ajou Univ
Indiana Univ	Deakin Univ	**Taif Univ**	Simplan	Xian Univ Technol
Univ Texas Dallas	Umm Al Qura Univ	Umm Al Qura Univ	Social Engn Acad	Carnegie Mellon Univ
Northeastern Univ	Birmingham City Univ	Univ New South Wales	Tuv Hellas Tuv Nord Sa	Univ Macau
Kobe Univ	Sci Inst Publ Law	Univ Patras	Univ Fed Rio De Janeiro	Univ Illinois
Univ Rijeka	St Petersburg State Univ	Univ Politecn Cataluna	Wayne State Univ	Natl Assoc Insurance Commissioners
World Maritime Univ	Waterford Inst Technol	North Carolina A&T State Univ	Serv Madriletio Salud	Telkom Univ
Suny Buffalo	Singapore Univ Technol & Design	Florida Int Univ	Atos Res & Innovat	Police Forens Lab Ctr
Inst Rural Management Anand Irma	Univ Fuerzas Armadas Espe	Univ West Florida	Natl Univ Sci & Technol	Siemens Ag

instrumental in recovery efforts.

3. Conclusions

When we look at the results obtained in the study, it is possible to say that there are important determinations about the prominent institutions and research areas. In particular, on the 5 functions proposed by NIST: identifying prominent institutions, countries, research focuses, and determining the dominant actors in the five functions mentioned. Thanks to the information obtained, it can be said that it has been developed as a tool that can be used in directing the cooperation models that can be made at the point of R&D policy development.

Tables 14 and 15 show the current research and potential intellectual property topics and domains in cybersecurity. Table 15 lists only the top 5 institutes identified in Tables 10–13. Different metrics are used in each table. Bolded institutes in Table 15 appear 5 or more times in the top 5 lists implying to be centers of research. They all appear to be in Saudi Arabia.

It is thought that the findings obtained in this context will contribute to all institutions and organizations that work on cyber security and make efforts in research and development activities. Following the main actors determined by the results obtained by cluster analysis and social network analysis, together with the method proposed in the study, can be used as a tool that will benefit the production of data-based policy in studies to be put forward in the field of cybersecurity. On the other hand, close monitoring of prominent subject areas, additionally nodal points with low constraints in capturing weak signals, can be used as a tool to identify points that are open to development and gain importance, and to closely monitor institutions and countries that will increase their importance.

Technology standards provide a foundation for intellectual property on which companies can build products and services. We are already seeing knowledge accumulating in this field. We expect the standards will ensure the protection of knowledge.

CRediT authorship contribution statement

Tugrul Daim: Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Haydar Yalcin:** Writing – original draft, Visualization, Formal analysis, Data curation, Conceptualization. **Alain Mermoud:** Writing – review & editing, Supervision, Project administration, Funding acquisition, Conceptualization. **Valentin Mulder:** Writing – original draft, Project administration, Conceptualization.

Declaration of competing interest

We have no conflicts of interest.

Data availability

Data will be made available on request.

Acknowledgement

This research was funded by the grant #8203005331 from Federal Department of Defence, armasuisse Science and Technology,

Switzerland.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.wpi.2024.102278.

References

[1] Ž. Turk, et al., A systemic framework for addressing cybersecurity in construction, Autom. ConStruct. 133 (2022) 103988.
[2] D.J. Ferreira, N. Mateus-Coelho, H.S. Mamede, Methodology for Predictive cyber security risk assessment (PCSRA), Proc. Comput. Sci. 219 (2023) 1555–1563.
[3] M.H. Rahman, T. Wuest, M. Shafae, Manufacturing cybersecurity threat attributes and countermeasures: review, meta-taxonomy, and use cases of cyberattack taxonomies, J. Manuf. Syst. 68 (2023) 196–208.
[4] K. Zenitani, *Attack graph analysis: an explanatory guide.* Computers & Security 126 (2023) 103081.
[5] G.K. Campbell, J.R. Hall II, Integrated Security System Definition, in: In Advances in Security Technology, Elsevier, 1987, pp. 17–31.
[6] M. Kounavis, et al., Security definitions, entropy measures and constructions for implicitly detecting data corruption, Comput. Commun. 160 (2020) 815–846.
[7] K. Rouibah, S. Ould-Ali, Dynamic data sharing and security in a collaborative product definition management system, Robot. Comput. Integrated Manuf. 23 (2) (2007) 217–233.
[8] V.V. Ribeiro, D.S. Cruzes, G.H. Travassos, Moderator factors of software security and performance verification, J. Syst. Software 184 (2022) 111137.
[9] I.A. Tøndel, D.S. Cruzes, Continuous software security through security prioritisation meetings, J. Syst. Software 194 (2022) 111477.
[10] F. Liu, C. Wu, X. Lin, A new definition of the contrast of visual cryptography scheme, Inf. Process. Lett. 110 (7) (2010) 241–246.
[11] K.Y. Yigzaw, et al., Roadmap to successful digital health ecosystems, Roadmap to Successful Digital Health Ecosystems (2022).
[12] M.J. Guitton, Cybersecurity, Social Engineering, Artificial Intelligence, Technological Addictions:: Societal Challenges for the Coming Decade, 2020.
[13] J.M. Hatfield, Social engineering in cybersecurity: the evolution of a concept, Comput. Secur. 73 (2018) 102–113.
[14] R. Sabillon, V. Cavaller, J. Cano, National cyber security strategies: global trends in cyberspace, Int. J. Comput. Syst. Sci. Eng. 5 (5) (2016) 67.
[15] G. Shukla, S. Gochhait, Cyber security trend analysis using Web of Science: a bibliometric analysis, Eur J Mol Clin Med 7 (6) (2020) 2567–2576.
[16] S. Kendzierskyj, H. Jahankhani, Critical national infrastructure, C4ISR and cyber weapons in the digital age, Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity (2020) 3–21.
[17] U.M. Mbanaso, J.A. Makinde, V.E. Kulugh, A methodological approach for characterisation of critical national infrastructure, Int. J. Crit. Infrastruct. 19 (2) (2023) 172–197.
[18] W. Harrop, A. Matteson, Cyber resilience: a review of critical national infrastructure and cyber security protection measures applied in the UK and USA, J. Bus. Continuity Emerg. Plan. 7 (2) (2014) 149–162.
[19] J.P.M.T. Dias, Increasing the Dependability of Internet-Of-Things Systems in the Context of End-User Development Environments, 2022.
[20] M. Tabassum, T. Kosinski, H.R. Lipford, I don't own the data": end user Perceptions of smart home device data Practices and risks, in Fifteenth symposium on usable privacy and security (SOUPS 2019) (2019).
[21] E. Zeng, S. Mare, F. Roesner, End user security and privacy concerns with smart homes, in: Thirteenth Symposium on Useable Privacy and Security (SOUPS 2017), 2017.
[22] B. Krumay, E.W. Bernroider, R. Walser, Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST cybersecurity framework, in: Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23, Springer, 2018.
[23] S. Shackelford, A. Boustead, C. Makridis, DEFINING "REASONABLE" CYBERSECURITY: LESSONS FROM THE STATES, 2021. Available at SSRN 3919275.
[24] C.E. Pascoe, Public Draft: The NIST Cybersecurity Framework 2.0. (2023).
[25] G. Marzi, et al., Product and process innovation in manufacturing firms: a 30-year bibliometric analysis, Scientometrics 113 (2017) 673–704.
[26] T.U. Daim, et al., Forecasting emerging technologies: Use of bibliometrics and patent analysis, Technol. Forecast. Soc. Change 73 (8) (2006) 981–1012.
[27] Y.-S. Su, et al., Assessing the technological trajectory of 5G-V2X autonomous driving inventions: use of patent analysis, Technol. Forecast. Soc. Change 196 (2023) 122817.
[28] S. Li, E. Garces, T. Daim, Technology forecasting by analogy-based on social network analysis: the case of autonomous vehicles, Technol. Forecast. Soc. Change 148 (2019) 119731.
[29] S. Li, et al., Measuring strategic technological strength: patent portfolio model, Technol. Forecast. Soc. Change 157 (2020) 120119.
[30] E. Garces, et al., Technology domain analysis: a case of energy-efficient advanced commercial refrigeration technologies, Sustain. Prod. Consum. 12 (2017) 221–233.
[31] T. Daim, et al., Time lag assessment between research funding and output in emerging technologies, Foresight 9 (4) (2007) 33–44.
[32] T.U. Daim, N. Gerdsri, Research and development progress assessment through technological and scientific intelligence, Int. J. Technol. Intell. Plann. 5 (4) (2009) 341–356.
[33] G. Zeba, et al., Technology mining: artificial intelligence in manufacturing, Technol. Forecast. Soc. Change 171 (2021) 120971.
[34] T.U. Daim, H. Yalçın, Digital Transformations: New Tools and Methods for Mining Technological Intelligence, Edward Elgar Publishing, 2022.
[35] T. Daim, et al., Forecasting technology trends through the gap between science and technology: the ?ase of software as an E-commerce service, Форсайт 15 (2021) 12–24, 2 (eng).
[36] H. Yalcin, T. Daim, Mining research and invention activity for innovation trends: case of blockchain technology, Scientometrics 126 (5) (2021) 3775–3806.
[37] H. Yalcin, T.U. Daim, Logistics, supply chain management and technology research: An analysis on the axis of technology mining, Transport. Res. E Logist. Transport. Rev. 168 (2022) 102943.
[38] M. Zamani, et al., Developing metrics for emerging technologies: identification and assessment, Technol. Forecast. Soc. Change 176 (2022) 121456.
[39] R.K. Blashfield, M.S. Aldenderfer, The literature on cluster analysis, Multivariate Behav. Res. 13 (3) (1978) 271–295.
[40] J.R. Kettenring, The practice of cluster analysis, J. Classif. 23 (2006) 3–30.
[41] M. Kampffmeyer, et al., Deep divergence-based approach to clustering, Neural Network. 113 (2019) 91–101.
[42] R. Kwon, et al., Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping, in: 2020 Resilience Week (RWS), IEEE, 2020.
[43] M. Scofield, Benefiting from the NIST cybersecurity framework, Inf. Manag. 50 (2) (2016) 25.
[44] L. Shen, The NIST cybersecurity framework: Overview and potential impacts, SciTech Lawyer 10 (4) (2014) 16.
[45] A. Calder, NIST Cybersecurity Framework: A Pocket Guide, IT Governance Publishing Ltd, 2018.
[46] A. Dedeke, Cybersecurity framework adoption: using capability levels for implementation tiers and profiles, IEEE Security & Privacy 15 (5) (2017) 47–54.
[47] B. Bokan, J. Santos, Managing cybersecurity risk using threat based methodology for evaluation of cybersecurity architectures, in: 2021 Systems and Information Engineering Design Symposium (SIEDS), IEEE, 2021.
[48] S. Cleveland, M. Cleveland, Toward cybersecurity leadership framework, in: Proceedings of the Thirteenth Midwest Association for Information Systems Conference, 2018.
[49] N.M. Radziwill, M.C. Benton, Cybersecurity cost of quality: managing the costs of cybersecurity risk management, arXiv preprint arXiv:1707.02653 (2017).
[50] E.C. Thompson, Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents, Apress, 2018.