

Applied Innovation and Technology Management

Tugrul U. Daim  
Marina Dabić *Editors*

# Cybersecurity


A Technology Landscape Analysis




Springer

# Applied Innovation and Technology Management

## Series Editors

Tugrul U. Daim , Department of Engineering & Technology Management  
Portland State University  
Portland, OR, USA

Marina Dabić , Faculty of Economics & Business  
University of Zagreb  
Zagreb, Croatia

Technology is not just limited to technology companies. Managing innovation and technology is no longer a luxury and needs to be understood by all sectors around the world and by both technical and non-technical managers. This book series explores existing and emerging technologies that address current challenges within innovation and technology managements. Each title is developed to provide a set of frameworks, tools and methods that can be adopted by researchers, managers and student in engineering, innovation and technology fields. Research, policy and practice-based books in the series cover topics such as roadmapping, portfolio management, technology forecasting, R&D management, health technologies, bio technologies, transportation management, smart cities, and open innovation, among many others.

Tugrul U. Daim • Marina Dabić  
Editors

# Cybersecurity

A Technology Landscape Analysis

 Springer

### *Editors*

Tugrul U. Daim   
Mark O. Hatfield Cybersecurity & Cyber  
Defense Policy Center  
Portland State University  
Portland, OR, USA

Marina Dabić   
Faculty of Economics and Business  
University of Zagreb  
Zagreb, Croatia  
  
University of Dubrovnik  
Dubrovnik, Croatia  
  
School of Economics and Business  
University of Ljubljana  
Ljubljana, Slovenia

ISSN 2662-9402

ISSN 2662-9410 (electronic)

Applied Innovation and Technology Management

ISBN 978-3-031-34842-6

ISBN 978-3-031-34843-3 (eBook)

<https://doi.org/10.1007/978-3-031-34843-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Contents

## Part I Technological Analyses

<b>1 Cybersecurity Technology: A Landscape Analysis</b> . . . . .	3
Mürsel Doğrul, Haydar Yalçın, and Tugrul U. Daim	
<b>2 Cybersecurity Technology: An Analysis of the Topic from 2011 to 2021</b> . . . . .	23
Yuliia Kyrdoda, Giacomo Marzi, Marina Dabić, and Tugrul U. Daim	
<b>3 Cybersecurity and Technology Convergence: Analysis of AI, Blockchain, and IoT Using SNA</b> . . . . .	39
Edwin Garces, Shuying Li, and Tugrul U. Daim	
<b>4 Patent Alert System.</b> . . . .	71
Alptekin Durmuşoğlu, Zeynep Didem Unutmaz Durmuşoğlu, and Tugrul U. Daim	

## Part II Strategic Analyses

<b>5 Technology Assessment of Cybersecurity</b> . . . . .	89
Hao Zhang and Tugrul U. Daim	
<b>6 Science and Technology Gap Analysis of Cybersecurity Technology</b> . . . . .	147
Xiaoli Wang, Xin Li, and Tugrul U. Daim	
<b>7 2030 Roadmap: Cybersecurity in Food E-Commerce.</b> . . . .	167
Cuong Nguyen, Jordan Wearing, Kawther Elolaimi, Pavithra Prasad, Prajakta Thorat, Tony Califano, and Tugrul U. Daim	

<b>8</b>	<b>Cybersecurity Technology Roadmap: Data and Information Security for Smart Grid Industry</b> . . . . .	<b>193</b>
	Anurag Yaddanapudi, Kaushik Chaudhary, Mohammad Alabdulaziz, Mohammed Albabtain, Nisha Hemantha Raju, Tasiya (Yaya) Sirimongkarakorn, Vijay Joshi, and Tugrul U. Daim	
 <b>Part III Sectoral Analyses</b>		
<b>9</b>	<b>Healthcare Information Systems Security Maturity Assessment</b> . . . .	<b>221</b>
	Bridget Barnes, Tugrul U. Daim, and Courtney Wright	
<b>10</b>	<b>Mapping the Knowledge of Cybersecurity in the Manufacturing Industry</b> . . . . .	<b>239</b>
	Gordana Zeba, Marina Dabić, Mirjana Čičak, Goran Vlašić, and Tugrul U. Daim	
<b>11</b>	<b>Technology Domain Analysis: Ecosystem for Proactive Cybersecurity in the Energy Sector</b> . . . . .	<b>267</b>
	Momtaz Khanam, Edwin Garces, Tugrul U. Daim, and Fayeze Alsoubaie	

# **Part I**

## **Technological Analyses**



# Chapter 1

## Cybersecurity Technology: A Landscape Analysis



Mürsel Doğrul , Haydar Yalçın , and Tugrul U. Daim

**Abstract** The focus of this chapter is to explore the impact of cybersecurity on the generation of knowledge and patents by analyzing the emergence of technological entrepreneurship and technological innovation within the state security environment. This topic is especially significant due to its dynamic ability to contribute to the national adoption of digital innovation by states. To produce and assess a fresh viewpoint on digital entrepreneurship driven by cybersecurity principles, pertinent data indicating the evolution of indicators for undertaking cybersecurity research in nations from 1999 to 2023 were analyzed. Examining cyberspace in-depth, this study employs bibliometric analysis as a methodology, as well as patent analysis, funding institutions, author productivity, institutional collaboration, institutional productivity, country collaboration, country productivity, and keyword analysis. Consequently, the rise of cybersecurity publications and patents is split into two categories: research and development (including startups, technological discoveries, and technology preparedness) and patents and trademarks (leveraging digital technology). This research reveals a number of strong correlations between these qualities, which contributes to the cybersecurity literature and has significant implications for corporate management and practitioners.

**Keywords** Security · Technology · Innovation · Research-funding institution · Patent · Saturation

---

M. Doğrul

Turkish National Defence University, Joint War Institute, Istanbul, Turkey

e-mail: [mdogrul@msu.edu.tr](mailto:mdogrul@msu.edu.tr)

H. Yalçın

Ege University, Division of Management Information Systems, Department of Business Administration, Faculty of Economics and Administrative Sciences, Izmir, Turkey

e-mail: [haydar.yalcin@ege.edu.tr](mailto:haydar.yalcin@ege.edu.tr)

T. U. Daim (✉)

Mark O. Hatfield Cybersecurity & Cyber Defense Policy Center, Portland State University, Portland, OR, USA

e-mail: [ji2td@pdx.edu](mailto:ji2td@pdx.edu)

## 1.1 Introduction

The primary focus of cybersecurity research in the past two decades has been on securing secure storage of personal information by states (Goutam, 2015). The rapidly changing and evolving nature of cyberspace has also led to its perception of insecurity (Choucri, 2014; Corn, 2017). With the advancement of technology, battlegrounds are no longer limited to physical borders, but also extend to digital spaces. Cybercrime is a significant threat to individuals, businesses, organizations, and governments (Bajpai, 2022; PwC, 2022). According to publicly available data, commercial email intrusions are expected to cost businesses \$43 billion between 2016 and 2021 (FBI, 2022).

To address this flaw, the concept of security has been developed, and traditional threat perceptions have been expanded to include the digital environment (Tan, 2021) and titled non-traditional security (NTS) (Mallavarapu, 2009). Security concerns have transitioned from the military to the civilian sphere, introducing new arguments and notions. Cyberattacks on power plants and pipelines have expanded the scope of cybersecurity to include energy security (Hoffmann, 2020; Malhotra et al., 2021)). It is currently more crucial than ever to take safeguards against the threats posed by cyberattacks. In April 2022, cybersecurity authorities from the United States, Australia, Canada, New Zealand, and the United Kingdom launched a joint Cybersecurity Advisory (CSA) proclamation against the backdrop of the ongoing war between Russia and Ukraine (CISA, 2022).

States strive to carefully preserve their citizens' data and prevent digital instability in the face of not just political crises such as war, but also highly advanced technology developments and societal demands (Doğrul & Erğürüm, 2021; Jafari-Sadeghi et al., 2021). States are compelled to leverage technology-producing infrastructures and corporations in order to maintain a substantial presence and offer security in the expanding and partially unregulated cosmos of cyberspace.

In this respect, by analyzing the concepts and keywords of cybersecurity, it is possible to anticipate the principal concerns of governments and the emergence of new areas of cybersecurity competition. By identifying crucial cybersecurity companies, their internationalization and even participation in international politics could be questioned. It can assess whether research-funding institutions around the world are also concerned with cybersecurity. It is possible to examine the global situation of the number of patents produced in cybersecurity and the internationalization performance of the companies that have them. In the context of cybersecurity, it is feasible to trace the intensity of investment in areas of expanding significance and the saturation levels of the concepts. Thus, the scholarly literature will be updated with the most recent trends, pillars, content, and advancement in cybersecurity technology.

## 1.2 Data and Method

In order to answer abovementioned questions and understand the basic and current features of the cybersecurity field, we preferred to conduct a bibliometric analysis. For this reason, we conducted an online search of the leading indices of the Web of Science (WoS). As a result of the query, bibliographic data of a total of 17,828 scientific publication documents between the years 1999 and 2023 were accessed. While a total of 34,841 authors contributed to the cybersecurity literature, where the annual growth rate was calculated as 5.36, 2874 of the publications contributed by these authors were single-authored. While there are 3.3 authors per document, 21.1% of the publications are the result of international collaboration.

In this study, the bibliometric analysis will reveal the intellectual structure and research concentration of cybersecurity. Bibliometrics is the application of mathematical and statistical techniques to scientific communication (Pritchard, 1969). Bibliometry can also be defined as a tool that has been developed for the quantitative evaluation of scientific literature and offers methods for research on the structure of scientific communication on scientific communication (Borgman & Furner, 1990). The first applications using the bibliometric method can be traced back to the early 1900s (Lawani, 1981; Thanuskodi, 2010). Since the 1970s, the importance of knowledge and knowledge management in every field has made bibliometrics, which is an important tool in the evaluation of scientific knowledge, a more frequently used method. Bibliometrics can be used at different scales for various purposes. In the analyses made by the authors (Chen, 2003; Fleming & Spicer, 2014; Glänzel & de Lange, 2002; Peters & Van Raan, 2005) while evaluating the collaborations in the field and the dissemination of scientific knowledge related to it (Glänzel & Schubert, 2005) and in the analyses made on keywords (Ding & Li, 2010; Liu et al., 2014; Muñoz-Leiva et al., 2012), the intellectual structure of scientific disciplines is revealed; time-dependent change or connection networks between sub-research fields can be seen (He & Yu, 2020). In the context of the application of bibliometric analysis at different scales, there are studies on the evaluation of authors' publications with citation analysis or co-word analysis in the microdimension, institutional evaluations in medium-sized studies, and the evaluation of the country or research area in the macrodimension (Chen, 2003). Open-source bibliographic databases will be used to obtain the data to be used in the project. Databases such as WoS, Scopus, and Google Scholar are frequently used in the bibliometric literature. The fact that Google Scholar is open to manipulation (Delgado López-Cózar et al., 2012; Labbé, 2010) may affect the reliability of the analysis. Although the Scopus database indexes more journals in terms of scope, the WoS bibliographic database will be used because the database is more inconsistent than WoS (Franceschini et al., 2016; Wang & Waltman, 2016). In this sense, the categories created by the WoS database in line with the research focus of the journals will be used to obtain data on sociology and the publications under the cybersecurity technologies analyzed.

### 1.2.1 *The Social Network Analysis (SNA)*

The SNA method was used to determine the subject areas and focal points in the field of cybersecurity. According to this, the frequency of each topic heading together was calculated, and then the values obtained were used in the calculation of social network metrics. To give information about the indicators, we use to determine the roles of the nodes in the network in social network analysis: Betweenness centrality is based on the shortest paths in a network. Betweenness is important for flows in a network. If a node with a high degree of betweenness is eliminated, it means that flows in this network will not be efficient, as the average of the shortest paths will increase (Scott, 2012, p. 114). Degree centrality relates to the number of first-order neighbors a node is connected to by a single link. Degree centrality is measured by the number of connections of a node, and this measure measures degree centrality in absolute terms (Bródka et al., 2012). Degree centrality concerns nodes that are first-degree neighbors of a node. However, there are also nodes that are indirectly linked to a node. Closeness centrality focuses on distance and takes into account nodes in indirect connection. Closeness is the average length of the shortest paths between a node and all other nodes in the graph. Proximity can be interpreted as the average access time, provided that access is provided from the shortest paths (Otte & Rousseau, 2002).

## 1.3 Keyword Analysis

Keyword analysis in bibliometrics is the act of discovering and analyzing the most frequently occurring words and phrases in a collection of papers or publications. It is often used to identify trends and patterns in research, to understand the most important topics being studied in a particular field, and to inform the development of research agendas. It can also be used to identify gaps in the research literature and to identify key influencers or leaders in a particular field.

When we look at the keyword analysis, we have looked at the nodes with a high ratio between the level of connectivity, the centrality of betweenness, and the level of closeness centrality, as well as the nodes where we can catch weak signals. Here, when we carry out the structural hole analysis application, which is one of the most important sub-analysis methods of social network analysis, we have determined the nodal points that have reached a certain level of saturation in terms of the technology growth phase and the technology sub-domains that are relatively more mobile in the network and open to development and can be defined as virgin areas. When we examine Table 1.1 closely, we see that especially the security model Internet framework status and management keywords are the nodal points with the highest values in terms of both the connection level and the center and proximity centers. On the other hand, when we look closely at the concepts that have reached the level of technological maturity, it is possible to say that the concept of impact, model,

**Table 1.1** Keyword analysis

All degree partition	Betweenness centrality	All closeness centrality	High aggregate constraints	Low aggregate constraints
Security	Security	Security	Impact	Ontology
Model	Model	Model	Model	Things security
Internet	Internet	Internet	Information security	Fake news
Framework	Framework	Framework	Cybersecurity	Attribution
Management	Management	Management	Decision-making	Observability
Systems	Systems	Systems	Performance	Representation
Impact	Impact	Impact	Information	Stock market
Challenges	Information	Challenges	Management	Placement
Cybersecurity	Challenges	Cybersecurity	Models	Level
Privacy	Cybersecurity	Privacy	Efficiency	Stochastic model
System	Attacks	Information	Power	Situation awareness
Information	Privacy	System	Behavior	C systems
Attacks	Performance	Cybersecurity	Technology	Offense
Performance	System	Attacks	Dynamics	Telehealth
Design	Design	Performance	Time	Support vector machine
Technology	Technology	Design	Knowledge	Watermarking
Networks	Cybersecurity	Technology	Cyber-security	Foundations
Risk	Networks	Networks	Strategies	Extraction
Cybersecurity	Risk	Risk	Framework	Architectures
Things	Behavior	Cyber-security	Risk	Art
Behavior	Cybersecurity	Things	Design	Set
Cybersecurity	Information security	Behavior	Determinants	Supervisory control
Future	Network	Information security	Security	Feedback
Network	Trust	Intrusion detection	Decision	Information security investment
Trust	Things	Network	Strategy	Children

information security, cybersecurity, decision-making, performance, information management, and model has now reached the level of technological saturation and has strengthened its position for the cybersecurity network. When we look at the key concepts that are open to development in terms of cybersecurity technologies and cyber defense technologies, it is possible to say that ontologies, the Internet of things, the concept of security in the Internet of things, the fake news phenomenon, the observability principle, and the re-representation principles are still among the nodal points that are open to development.

When keyword analysis is evaluated within itself, the search for models continues. There are different levels of saturation. The overlooked and untouched topics (potential) are topics such as “children,” the “stock market,” and the “things

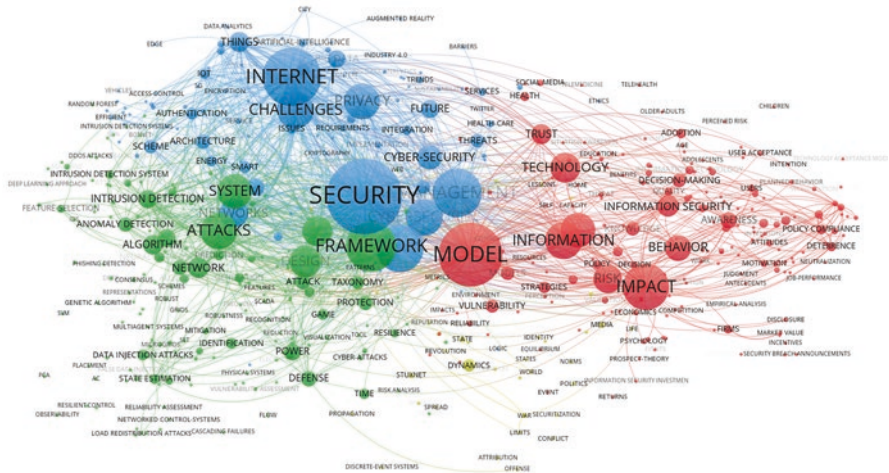


Fig. 1.1 Interaction map of research fields and keywords

security.” Interestingly, “fake news” has not yet emerged as a prioritized topic in the cybersecurity space. This can also be considered an explanation for the lack of measures taken in the face of today’s information pollution.

When the interaction map (Fig. 1.1) of the keywords of scientific publications on cybersecurity with other concepts in the studies is examined, it is seen that the concepts of “Internet,” “security,” “model,” “impact,” “framework,” “attack,” “information,” and “challenges” stand out. In addition, “security,” “Internet,” “model,” “information,” “technology,” and “trust” are interacting keywords. At the common interaction point of all studies, the concepts of “management,” “model,” “protection,” and “privacy” can be seen. The keywords “power,” “defense,” “framework,” and “security” interact with “Internet,” “information,” and “cybersecurity” in a side cluster. These keywords also overlap with the contemporary contexts of security studies in international relations (Routledge, 2023).

### 1.4 Country Productivity

According to the results of the country productivity (Table 1.2) analysis we have done, we see that the United States is at the top of the list above China and England, unlike the results we have achieved in other technology domain studies in terms of both the number of documents and the number of citations received when evaluated together with performance indicators, the number of publications, and the number of citations. Considering the h-index, which represents the intersection point, we see that the United States is at the top of the list with a value of 122. While China is at the second place, then the United Kingdom, Australia, Canada, India, Italy, Spain, and Pakistan are at the top of the list, while Türkiye also contributes with 350

**Table 1.2** Country productivity

Country	Citation sum within h-core	All citations	All documents	h-index
USA	30,959	111,959	10,909	122
Peoples R China	12,653	32,505	2653	82
UK	9254	25,065	2324	68
Australia	7464	16,993	1349	61
Canada	5069	10,313	997	46
India	5116	11,492	1566	46
Italy	4080	8790	997	41
Spain	3212	6938	784	36
Pakistan	2467	4228	367	35
Singapore	2805	4166	314	34
South Korea	2418	5695	731	33
Turkey	2616	3890	357	32
Sweden	2836	4099	310	31
Japan	2057	4116	592	30
Saudi Arabia	1950	4826	785	29
France	1575	3609	656	26
Germany	1660	3951	841	25
Netherlands	1894	3304	365	24
Taiwan	1033	1829	256	24
Norway	1400	2688	406	24
Poland	812	1941	393	24
Denmark	1610	2183	137	22
Greece	950	2557	432	22
Malaysia	1092	2229	399	21
Israel	988	1777	252	21

publications, both in terms of the number of publications and the total number of citations received. It is possible to see that it has taken an important place on the list.

1.5 Country Collaboration

Table 1.3 presents the cooperation of various countries in the study. The analysis of the network reveals that the United States is the leading country in all three values, followed by the United Kingdom. Upon examining the countries with the highest level of maturity in cybersecurity research, particularly in terms of high connectivity in the network, it is evident that the United States, United Kingdom, India, China, Gambia, Australia, and Paraguay are among the top performers. On the other hand, the Czech Republic, Slovenia, Denmark, Estonia, and the United Arab Emirates are among the countries with relatively fewer connections in the country cooperation network, as measured by country connectivity levels. Notable also is

**Table 1.3** Country collaboration

All degree partition	Betweenness centrality	All closeness centrality	Aggregate constrain HAC	Aggregate constraint LAC
USA	USA	USA	Jamaica	Czech Republic
UK	UK	UK	USA	Slovenia
India	Australia	India	UK	Denmark
Peoples R China	India	Peoples R China	India	Estonia
Australia	Peoples R China	Australia	Peoples R China	U Arab Emirates
Spain	Spain	Canada	Gambia	Vietnam
Saudi Arabia	Saudi Arabia	Saudi Arabia	Australia	Saudi Arabia
Germany	Germany	Spain	Paraguay	Poland
France	South Africa	Germany	Bhutan	Thailand
Canada	Canada	Italy	Canada	Ghana
Italy	Russia	Norway	Saudi Arabia	Norway
Norway	France	France	Spain	Spain
Pakistan	Ukraine	Malaysia	Germany	Iraq
Netherlands	Hungary	Poland	Mozambique	Finland
South Korea	Italy	Pakistan	Italy	Iran
Malaysia	Turkey	Czech Republic	Norway	UK
Czech Republic	Malaysia	South Korea	France	Netherlands
Poland	Norway	Netherlands	Malaysia	Pakistan
Turkey	Iran	Turkey	South Korea	Nigeria
Sweden	Belgium	Sweden	Pakistan	Jordan
Finland	Japan	Switzerland	Poland	Belgium
Greece	Poland	Finland	Czech Republic	Slovakia
Portugal	Uganda	U Arab Emirates	Netherlands	Ireland
Japan	Pakistan	Japan	Turkey	Switzerland
Taiwan	Czech Republic	Taiwan	Sweden	Sweden

the fact that Saudi Arabia has a high ranking in all degree of partition, betweenness centrality, and closeness centrality, allowing it to be included among the G-7 nations in this table.

## 1.6 Institutional Productivity

When we look at institutional productivity and contribution (Table 1.4), it is seen that Carnegie Mellon University; University of California, Berkeley; New York University (NYU); the University of Texas San Antonio; MIT; and the University of California are at the top of the list. It is possible to say that MIT is at the top of the list in terms of the number of publications, but when we consider it in terms of the intersection of the number of publications and the number of citations, that is, in



**Table 1.4** Productivity of the institutions

Institution	Citation sum within h-core	All citations	All documents	H-index
Carnegie Mellon Univ	3008	3490	151	22
Univ Calif Berkeley	2120	2277	54	21
NYU	988	1357	117	21
Univ Texas San Antonio	994	1779	150	21
MIT	1084	1490	170	20
Univ Oxford	922	1347	131	20
Virginia Tech	814	1219	101	20
Arizona State Univ	778	1172	103	20
Swinburne Univ Technol	1035	1179	49	19
Singapore Univ Technol and Design	1057	1229	59	19
Tsinghua Univ	1260	1521	83	18
Univ Arizona	680	1024	83	18
Iowa State Univ	2598	2811	83	18
Univ Virginia	869	1151	77	18
Washington State Univ	926	1214	72	18
Texas A & M Univ	1240	1448	89	17
Deakin Univ	838	1187	99	17
IIT (Illinois Institute of Technology	925	1051	46	17
Univ Toledo	1267	1410	80	17
Purdue Univ	477	846	130	17
Univ Michigan	732	973	77	17
Univ Illinois	869	1213	116	17
Georgia Inst Technol	932	1144	74	16
King Saud Univ	908	1341	104	16
Univ Waterloo	1413	1580	52	16

terms of the h-index, it is possible to say that the list is formed in the axis of the order mentioned before. A number of universities in the United States are ranked higher than Tsinghua University, a prestigious university in China when it comes to the productivity of cybersecurity studies.

1.7 Institutional Collaboration

In terms of institutional cooperation (Table 1.5), it is possible to see that Carnegie Mellon University and Berlin University are at the top of the list in terms of connectivity, while University Texas San Antonio is at the top of the list in terms of centrality betweenness. When we look at the indicator of being in close relationship with other nodes, that is, in terms of closeness centrality, we see that Carnegie

**Table 1.5** Collaboration of the institutions

<b>All degree partition</b>	<b>Betweenness centrality</b>	<b>All closeness centrality</b>	<b>Aggregate constraint HAC</b>	<b>Aggregate constraint LAC</b>
Carnegie Mellon Univ	Univ Texas San Antonio	Carnegie Mellon Univ	Carnegie Mellon Univ	Tsinghua Univ
Univ Texas San Antonio	King Saud Univ	Univ Texas San Antonio	Univ Texas San Antonio	Shanghai Jiao Tong Univ
MIT	Carnegie Mellon Univ	Univ Illinois	Univ Illinois	Delft Univ Technol
Univ Illinois	Tsinghua Univ	MIT	MIT	Nanyang Technol Univ
Univ Oxford	Univ Oxford	Univ Oxford	Univ Oxford	Univ Texas San Antonio
King Saud Univ	MIT	Univ New South Wales	Nanyang Technol Univ	Univ Michigan
Univ New South Wales	Univ Illinois	Nanyang Technol Univ	Tsinghua Univ	Kings Coll London
Nanyang Technol Univ	Univ New South Wales	Tsinghua Univ	Univ Michigan	Aalborg Univ
Penn State Univ	King Abdulaziz Univ	Shanghai Jiao Tong Univ	Delft Univ Technol	Univ Texas Austin
Univ Michigan	Delft Univ Technol	Harvard Univ	King Saud Univ	Univ New South Wales
Delft Univ Technol	Norwegian Univ Sci & #38; Technol	Univ Michigan	Penn State Univ	Univ Calif Los Angeles
Harvard Univ	Nanyang Technol Univ	Delft Univ Technol	Purdue Univ	Univ Alberta
Univ Southern Calif	Univ Calif Berkeley	King Saud Univ	Indiana Univ	Univ Oxford
Deakin Univ	Univ Michigan	Penn State Univ	Univ Southern Calif	Macquarie Univ
George Mason Univ	George Mason Univ	Chinese Acad Sci	Imperial Coll London	Univ Calif Berkeley
Univ Calif Berkeley	Univ S Florida	Purdue Univ	Univ Calif Berkeley	North Carolina State Univ
Purdue Univ	Univ Waterloo	Indiana Univ	Royal Inst Technol	Norwegian Univ Sci & #38; Technol
Univ Tennessee	Deakin Univ	Norwegian Univ Sci & #38; Technol	King Abdulaziz Univ	Univ Technol Sydney
Univ Minnesota	Imperial Coll London	Univ Southern Calif	George Mason Univ	Univ Minnesota
Univ Waterloo	Univ Strathclyde	Imperial Coll London	Arizona State Univ	Tennessee Technol Univ
Norwegian Univ Sci & #38; Technol	Arizona State Univ	Univ Calif Berkeley	Univ Calif Los Angeles	US Army

(continued)

Table 1.5 (continued)

All degree partition	Betweenness centrality	All closeness centrality	Aggregate constraint HAC	Aggregate constraint LAC
Chinese Acad Sci	Kings Coll London	Univ Texas Austin	Univ Toronto	Natl Univ Singapore
Tsinghua Univ	Univ Arizona	King Abdulaziz Univ	Kings Coll London	Univ Massachusetts
Macquarie Univ	Penn State Univ	Univ Waterloo	Univ S Florida	Penn State Univ
Shanghai Jiao Tong Univ	Virginia Tech	George Mason Univ	NYU	Florida Int Univ

Mellon University is at the top of the list. In other words, it can be said that the maturity level of Carnegie Mellon University is quite high. When we look at the institutions that are open to development and have a more flexible structure in terms of developing institutional cooperation, it can be said that Tsinghua University, Shanghai Jiao Tong University, and Delft University of Technology institutions are at the top of the list.

1.8 Author Productivity

Table 1.6 shows the productivity of the Authors. Chen-Ching Liu from Virginia Polytechnic Institute and State University topped the list with 33 publications and 15 h-index, Soman K P from Amrita Vishwa Vidyapeetham University in India ranked second with 20 publications and 13 h-index, and Manimaran Govindarasu from Iowa State University ranked third with 38 publications and 13 h-index. In addition, according to Table 1.6, it is seen that productive researchers are mostly from US universities.

1.9 Funding Institutions

The funding institutions for cybersecurity studies and their publication/citation indication are listed in Table 1.7. China’s National Natural Science Foundation ranks first with 397 articles and an h-index of 42. With 323 publications and a 32 h-index, the National Science Foundation in the United States is the second most productive and successful institution in terms of funding. EPSRC Funding Source (UKRI) ranks third with 99 articles and an h-index of 25. The EU and its project titles, such as Horizon (Press release, 2022), are also on the list, and in recent years, cybersecurity has been given high priority in the project titles. Institutions from Korea, Japan, and other Asian nations are also included in the list. The presence of

**Table 1.6** Productivity of the authors

Author	Citation sum within h-core	All citations	All articles	h-index
Liu, Chen-Ching	1239	1315	33	15
Soman, K. P	941	982	20	13
Govindarasu, Manimaran	1699	1787	38	13
Alazab, Mamoun	980	1033	26	13
Ishii, Hideaki	647	717	28	12
Xu, Shouhuai	319	380	29	12
Chen, Hsinchun	310	397	30	12
Zhang, Jun	633	676	24	12
Choo, Kim-Kwang Raymond	489	545	33	12
Xiang, Yang	574	628	25	11
Wang, Lingfeng	693	741	47	11
Poornachandran, Prabakaran	884	912	16	11
Qiu, Meikang	711	748	20	11
Wang, Jianhui	931	953	15	11
Joshi, Anupam	312	405	32	11
Sengupta, Shamik	163	215	29	10
Janicke, Helge	749	806	31	10
Zhu, Quanyan	292	346	28	10
Kwiat, Kevin A	249	249	10	10
Hammoudeh, Mohammad	221	247	15	9
Debbabi, Mourad	258	283	17	9
Lu, Rongxing	1015	1016	10	9
Vinayakumar R	834	843	11	9
Pan, Lei	223	240	15	9
Hahn, Adam	983	1015	15	9

nearly all of the world's most prestigious funding institutions on this list indicates that cyberspace and security will continue to gain relevance in the future.

## 1.10 Patent Analysis

Emerging technology refers to technologies that are currently under development or in the early stages of adoption and distribution. These technologies have the potential to significantly impact and disrupt the way we live and work. Among emerging technologies, a number of new technologies such as artificial intelligence, virtual reality, blockchain, and the Internet of things (IoT) are affecting all areas where they are associated with their innovative and potentially transformative nature. In this respect, a better understanding of cybersecurity technologies, which are associated with a high level of uncertainty and risk, through the inferences to be obtained with patent data can be turned into an advantage in the context of technology management.

**Table 1.7** Institutions providing funding for cybersecurity research and publication/citation indicator

Unit	Citation sum within h-core	All citations	All articles	h-index
National Natural Science Foundation of China	3377	5405	397	42
National Science Foundation	3493	5017	323	32
EPSRC Funding Source: UKRI	2033	2588	99	25
NSF	1841	2591	187	21
US National Science Foundation	1705	1836	53	17
Engineering and Physical Sciences Research Council Funding Source: researchfish	1323	1389	24	16
National Key Research and Development Program of China	735	934	84	16
European Commission	431	557	58	15
Department of Energy	595	713	58	15
National Science Foundation of China	564	628	35	14
National Science Foundation (NSF)	910	1088	73	13
European Union	428	793	184	13
Fundamental Research Funds for the Central Universities	983	1125	47	13
Office of Naval Research	333	419	45	13
ARO	268	343	30	12
Division Of Computer and Network Systems Funding Source: National Science Foundation	897	911	15	11
US National Science Foundation	294	332	32	11
Army Research Office	326	391	36	11
Direct For Computer & Info Scie & Enginr Funding Source: National Science Foundation	1167	1187	15	10
US Department of Energy	596	680	38	10
National Key R & D Program of China	753	831	47	10
Natural Sciences and Engineering Research Council of Canada	385	389	12	9
Fundamental Research Funds for the Central Universities	323	328	14	9
Australian Research Council	332	360	15	9
Natural Science Foundation of China	1030	1074	23	9
European Union's Horizon 2020 research and innovation programme	202	249	37	8
China Postdoctoral Science Foundation	296	309	21	8
National Research Foundation of Korea	125	137	15	8
Australian Government Research Training Program Scholarship	149	149	9	8
National Science Foundation (NSF), USA	87	118	17	7
National Natural Science Foundation of China (NSFC)	393	420	25	7
Xunta de Galicia	542	558	10	7

(continued)

**Table 1.7** (continued)

Unit	Citation sum within h-core	All citations	All articles	h-index
Agencia Estatal de Investigacion of Spain	542	554	9	7
JSPS	334	336	8	7
Qatar National Research Fund (QNRF)	210	220	10	7
JSPS KAKENHI	176	217	33	7
Paramount Computer Systems	587	593	7	6
EU	171	213	32	6
NSFC	109	126	19	6

Among the technology classes with the highest level of connectivity (all degree partition) are H04L63 (network architectures or network communication protocols for network security) and H04L67 (network arrangements or protocols for supporting network services or applications). B42D25 (information-bearing cards or sheet-like structures characterized by identification or security features) and G01N23 (investigating or analyzing materials by the use of wave or particle radiation) stand out in terms of technology classes that are most open to development (low aggregate constraint). When we detect technology that has reached saturation level with structural hole analysis, we can also classify it as H04B1 (details of transmission systems, not covered by a single one of groups H04B 3/00 - H04B 13/00; details of transmission systems not characterized by the medium used for) and H02J7 (circuit arrangements for charging or depolarizing batteries or for supplying loads from batteries) (Table 1.8).

In this context, we aimed to identify the technology areas that have reached saturation through the patent registration efforts of cybersecurity technologies, which are seen to be at the focal point of important investments and research and the sub-technology areas that are open to development and still remain untouched. For this purpose, a concept network map was developed by determining the interrelationships of technology classes by using social network analysis and structural hole analysis together (Fig. 1.2).

Table 1.9 presents the list of companies conducting research, projects, and patent work in the field of cybersecurity, as well as their patent and citation values. FireEye, Inc. (California/USA) ranks first with 132 patents and 45 h-index. It is followed by Palantir Technologies from the United States with 339 patents and 42 h-index. In third place is Cilag GmbH International from Switzerland with 125 patents and a 40 h-index. The rest of the list includes well-known international large technology and innovation companies such as HP and Boeing. Following universities, research, and funding institutions, the companies on this list have also been seen to be moving into cyberspace and taking action. In fact, their success in this field further contributes to their internationalization. They find it as important to protect their products from malware as it is to produce robotics and high-tech products. Finally, a company's high number of patents does not always bring with it the impact of the patent. For example, although US-based IBM (International Business Machines

**Table 1.8** Social network analysis on patent data

All degree partition	Weighted all degree	Betweenness centrality	Low aggregate constraint	High aggregate constraint
H04L63	H04L63	H04L63	B42D25	H04B1
H04L67	H04L67	H04L67	G01N23	H02J7
G06F21	G06F21	G06F3	G01N2223	G06V20
G06Q50	G06Q50	G06F21	H04L63	G06K7
H04W4	H04W4	G06Q10	A61B2017	G01N33
H04L9	H04L9	H04L9	G06F16	G06F1
G06Q10	G06Q10	G06Q50	H04L9	G08B21
G06F3	G06F3	H04W4	G06N3	H04W84
G05B2219	G05B2219	G05B2219	H04L41	G06Q10
G06N20	G06N20	G06N3	G06F3	H04Q2209
G06N3	G06N3	G08B13	G06Q10	G08B5
G06F16	G06F16	G06F16	G06F11	B60W60
H04W12	H04W12	G05B19	G06Q20	G01N21
G06Q30	G06Q30	G06N20	A61B5	H04N7
G05B19	G05B19	G16H40	H04N21	H04W8
H04L41	H04L41	H04L41	G06F9	H02J9
H04L12	H04L12	H04L12	G01S13	H04N5
G06N5	G06N5	H04B10	H04B7	G06K19
H04W84	H04W84	H04W12	H05B47	Y04S40
G06F11	G06F11	G06F9	A61B6	G06F3
H04L43	H04L43	G06F1	A61M2205	B60W2556
G06F2221	G06F2221	G06Q30	G06F2212	G01S19
G06F9	G06F9	Y04S40	G06F8	G06Q50
Y04S40	Y04S40	H04W84	H02J13	A61B5
G16H40	G16H40	G09F3	G08B13	G16H10

Corporation) has 600 patents, the impact value of the company’s patents is displayed as 22. Thus, it is understood that Table 1.8 also contains information about cyberspace companies that are lagging behind in the competitive process and in need of innovative research through the number of patents.

1.11 Conclusion

The expanding definition of security, particularly in the digital realm, has become more prominent in recent studies. There has been a linear increase in the number of studies addressing cybersecurity in the context of national and international security. However, the critical level reached by technologies in the field of cybersecurity has shown that the area has not yet reached saturation in terms of publications and patents. There is a direct relationship between the success of patent applications and





**Table 1.9** The name of the production companies and patent information

Owners	Citation sum within h-core	All citations	All patents	h-index
FireEye, Inc.	6138	6762	132	45
Palantir Technologies Inc.	5447	6779	339	43
Cilag GmbH International	3972	4460	125	40
Ethicon LLC	3799	4279	123	39
Splunk Inc.	1949	2870	113	30
Onetrust LLC	2152	2271	189	28
Hewlett-Packard Development Company L.P.	8523	8833	83	28
Autoconnect Holdings LLC	2626	2851	48	26
Flextronics AP, LLC	2626	2848	45	26
Johnson Controls Technology Company	3153	3368	61	24
The Boeing Company	1837	2367	169	23
General Electric Company	1176	1704	147	22
International Business Machines Corporation	1135	2513	600	22
Hewlett Packard Enterprise Development LP	7942	8071	56	21
Strong Force IoT Portfolio 2016 LLC	1778	2370	168	21
Intralinks, Inc.	2621	2710	30	20
Proofpoint Inc.	1690	1787	66	20
ALTR Solutions, Inc.	858	1049	62	19
Wombat Security Technologies, Inc.	1511	1544	29	18
VeriFone, Inc.	7522	7522	17	17
Hewlett-Packard Company	7522	7522	17	17
Pure Storage, Inc.	435	903	283	16
Security Scorecard, Inc.	643	651	21	16
Honeywell International Inc.	721	1059	177	16
Bromium, Inc.	741	861	43	15

## References

- Bajpai, P. (2022). An overview of the cybersecurity landscape and ways to invest in the space. Nasdaq. <https://www.nasdaq.com/articles/an-overview-of-the-cybersecurity-landscape-and-ways-to-invest-in-the-space>
- Borgman, C., & Furner, J. (1990). *Scholarly Communication and Bibliometrics*. Sage.
- Bródka, P., Skibicki, K., Kazienko, P., & Musiał, K. (2012). A degree centrality in multi-layered social network. *CoRR*, abs/1210.5184. <http://arxiv.org/abs/1210.5184>
- Chen, C. (2003). On the shoulders of giants. In *Mapping scientific frontiers: The quest for knowledge visualization* (pp. 135–166). Springer. [https://doi.org/10.1007/978-1-4471-0051-5\\_5](https://doi.org/10.1007/978-1-4471-0051-5_5)
- Choucri, N. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, 20(2), 96–121. <https://doi.org/10.1080/02681102.2013.836699>

- CISA. (2022). *Russian state-sponsored and criminal cyber threats to critical infrastructure*. <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a>
- Corn, G. P. (2017). Sovereignty in the age of cyber. *American Journal of International Law*, 111, 207–212. <https://doi.org/10.1017/AJU.2017.57>
- Delgado López-Cózar, E., Robinson García, N., & Torres Salinas, D. (2012). Manipular Google Scholar Citations y Google Scholar Metrics: Simple, sencillo y tentador. <http://hdl.handle.net/10481/20469>.
- Ding, Y., & Li, G. (2010). Study on the management of intellectual capital. *International Journal of Business and Management*, 5(2), 213–216.
- Doğrul, M., & Erğürüm, A. (2021). New Search for Cybersecurity in the Light of Blockchain's Literature Expansion (Blok Zincirinin (Blockchain) Literatür Büyümesi Işığında Yeni Siber Güvenlik Arayışları). *Güvenlik Bilimleri Dergisi*, 10(3), 3. <https://doi.org/10.28956/gbd.1016087>
- FBI. (2022). *Internet Crime Complaint Center (IC3) Business Email Compromise: The \$43 Billion Scam*. Alert Number: I-050422-PSA. <https://www.ic3.gov/Media/Y2022/PSA220504>
- Fleming, P., & Spicer, A. (2014). Power in management and organization science. *The Academy of Management Annals*, 8(1), 237–298. <https://doi.org/10.1080/19416520.2014.875671>
- Franceschini, F., Maisano, D., & Mastrogiacomo, L. (2016). The museum of errors/horrors in Scopus. *Journal of Informetrics*, 10(1), 174–182. <https://doi.org/10.1016/j.joi.2015.11.006>
- Glänzel, W., & de Lange, C. (2002). A distributional approach to multinationality measures of international scientific collaboration. *Scientometrics*, 54(1), 75–89. <https://doi.org/10.1023/A:1015684505035>
- Glänzel, W., & Schubert, A. (2005). Analysing Scientific networks through co-authorship. In H. F. Moed, W. Glänzel, & U. Schmoch (Eds.), *Handbook of quantitative science and technology research: The use of publication and patent statistics in studies of S & T systems* (pp. 257–276). Springer. [https://doi.org/10.1007/1-4020-2755-9\\_12](https://doi.org/10.1007/1-4020-2755-9_12)
- Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, 111(7), 14–17. <https://doi.org/10.5120/19550-1250>
- He, X., & Yu, D. (2020). Research trends in life cycle assessment research: A 20-year bibliometric analysis (1999–2018). *Environmental Impact Assessment Review*, 85, 106461. <https://doi.org/10.1016/j.eiar.2020.106461>
- Hoffmann, R. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, 44, 655–662. <https://doi.org/10.1016/J.PROMFG.2020.02.243>
- Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E., & Couturier, J. (2021). Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. *Journal of Business Research*, 124, 100–111. <https://doi.org/10.1016/J.JBUSRES.2020.11.020>
- Labbé, C. (2010). Ike Antkare one of the great stars in the scientific firmament. *International Society for Scientometrics and Informetrics Newsletter*, 6(2), 48–52.
- Lawani, S. M. (1981). Bibliometrics: Its theoretical foundations. *Methods Applications*.
- Liu, Y., Gonçalves, J., Ferreira, D., Xiao, B., Hosio, S. J., & Kostakos, V. (2014). CHI 1994–2013: Mapping two decades of intellectual progress through co-word analysis. In *Proceedings of the SIGCHI conference on human factors in computing systems*.
- Malhotra, P., Singh, Y., Anand, P., Deep Kumar, B., & Singh. (2021). Internet of things: Evolution. *Concerns and Security Challenges. Sensors*, 21(5), 5. <https://doi.org/10.3390/S21051809>
- Mallavarapu, S. (2009). *International Relations Theory and Non-Traditional Approaches to Security*. 84. <http://wiscomp.org/Publications/141%20-%20Perspectives%2027%20-%20International%20Relations%20Theory%20and%20Non-Traditional%20Approaches%20to%20Security.pdf>
- Muñoz-Leiva, F., Viedma-del-Jesús, M. I., Sánchez-Fernández, J., & López-Herrera, A. G. (2012). An application of co-word analysis and bibliometric maps for detecting the most highlighting themes in the consumer behaviour research from a longitudinal perspective. *Quality & Quantity*, 46(4), 1077–1095. <https://doi.org/10.1007/s11135-011-9565-3>

- Otte, E., & Rousseau, R. (2002). Social network analysis: A powerful strategy, also for the information sciences. *Journal of Information Science*, 28(6), 441–453. <https://doi.org/10.1177/016555150202800601>
- Peters, H. P. F., & Van Raan, A. F. J. (2005). Structuring scientific activities by co-author analysis. *Scientometrics*, 20, 235–255.
- Press release. (2022, November 10). Cyber defence: EU boosts action against cyber threats. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_22\\_6642](https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642)
- Pritchard, A. (1969). Statistical bibliography or bibliometrics. *Journal of Documentation*, 25, 348.
- PwC. (2022). PwC's global economic crime and fraud survey 2022; Protecting the perimeter: The rise of external fraud.
- Routledge. (2023). *Contemporary security studies—Book Series—Routledge & CRC Press*. <https://www.routledge.com/Contemporary-Security-Studies/book-series/CSS>
- Scott, J. (2012). *What is Social Network Analysis?* (1st ed.). Bloomsbury Collections. <https://doi.org/10.5040/9781849668187>
- Tan, L. (2021). Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness. *IEEE Consumer Electronics Magazine*, 1–1. <https://doi.org/10.1109/MCE.2021.3081874>
- Thanuskodi, S. (2010). Journal of social sciences: A bibliometric study. *Journal of Social Sciences*, 24(2), 77–80. <https://doi.org/10.1080/09718923.2010.11892847>
- Wang, Q., & Waltman, L. (2016). Large-scale analysis of the accuracy of the journal classification systems of Web of Science and Scopus. *Journal of Informetrics*, 10(2), 347–364. <https://doi.org/10.1016/j.joi.2016.02.003>

## Chapter 2

# Cybersecurity Technology: An Analysis of the Topic from 2011 to 2021



Yuliia Kyrdoda, Giacomo Marzi, Marina Dabić, and Tugrul U. Daim

**Abstract** The main purpose of the study is to present a bibliometric overview of the published research within the cybersecurity framework over the recent decade. The study applies bibliometric analysis in order to analyze the most relevant journals, authors, and countries, as well as the most cited papers between 2011 and 2021. We identified activity and relationship indicators about the distribution of articles over time, most-cited journals, and most relevant countries, co-author analysis, and keyword analysis.

Different classifications have been made, including an analysis of the most influential journal, the most cited papers, the most relevant authors, and countries with over 20 publications in the field over the last decade. Also, the analysis identified four leading topics: cybersecurity management, intrusion detection and prevention, smart grids, cybercrime and cyberattacks.

**Keywords** Cybersecurity · Bibliometric · Literature review · Keywords · VOS

---

Y. Kyrdoda

Department of Economics, Business, Mathematics, and Statistics “Bruno de Finetti”,  
University of Trieste, Trieste, Italy  
e-mail: [yuliia.kyrdoda@units.it](mailto:yuliia.kyrdoda@units.it)

G. Marzi

IMT School for Advanced Studies Lucca, Lucca, Italy  
e-mail: [giacomo.marzi@imtlucca.it](mailto:giacomo.marzi@imtlucca.it)

M. Dabić

Faculty of Economics and Business, University of Zagreb, Zagreb, Croatia

University of Dubrovnik, Dubrovnik, Croatia

School of Economics and Business, University of Ljubljana, Ljubljana, Slovenia

e-mail: [mdabic@net.efzg.hr](mailto:mdabic@net.efzg.hr)

T. U. Daim (✉)

Mark O. Hatfield Cybersecurity & Cyber Defense Policy Center, Portland State University,  
Portland, OR, USA

e-mail: [ji2td@pdx.edu](mailto:ji2td@pdx.edu)

## 2.1 Introduction

Nowadays, cybersecurity is getting more attention as the growing use of technologies demands more efficient information protection because of the high numbers of digital threats (Arora, 2016). Considering rapid changes toward digital solutions either on an individual and national level, developing cybersecurity technologies that can resist cyberattacks is a critical call for both practitioners and scholars.

Cybersecurity is a collection of resources, processes, and structures aiming to secure the cyber environment and property rights from potential hazards and mitigate cybersecurity incidents (Craig et al., 2014).

Prior research (Michael et al., 2019; von Solms & van Niekerk, 2013; Wang & Lu, 2013) pointed out the triangle model defining the primary objectives of cybersecurity as availability which relies on open access to the information, integrity encompassing correctness, the trustworthiness of the data, and confidentiality of the information. Thus, the breach of these pillars caused by cyberattacks might lead to dis-balance within the entire system.

While many studies have focused on the advancing technologies to solve safety issues within digital space (see as an example Thakur et al. (2015)), the abilities of cyberattacks to alternate the information were progressing as well (Uma & Padmavathi, 2013). Hence, important issues of cybersecurity literature include the comprehensive overview of the current situation within the cybersecurity domain by defining the main existing contributions of the research.

To address this call, the present study offers a thoughtful review of published papers over the last decade. In doing so, we applied bibliometric analysis which allows identifying current evidence in the literature along with future directions for the research by mapping and systematizing cybersecurity research for the period 2011–2021.

In line with the objectives of the study, the primary research question focuses on what the current state-of-the-art within the cybersecurity field is. We performed a comprehensive bibliometric and literature exploration comprising bibliometric activity indicators, such as distribution of articles over time, most-cited journals, and most relevant countries, and relationship indicators, such as co-author analysis and keyword analysis. The findings reveal four research themes based on the analysis of keywords, namely, cybersecurity management, intrusion detection and prevention, smart grids, and cyberattacks. Also, the results summarize future research directions.

The present study is structured as follows. The next paragraph presents the methods. Paragraph 3 presents the bibliometric analysis on the cybersecurity field, while paragraph 4 depicts the major studies included in the four emerging clusters of topics. Finally, paragraph 4 presents the conclusion and the future research avenues.