BALKAN JOURNAL OF ELECTRICAL & COMPUTER ENGINEERING, Vol. 14, 2026
Research Article

A Bibliometric Analysis of Maritime Cybersecurity: Trends, Themes, and Collaboration Patterns

Murat Koca[1]

***Abstract*— The rapid development and increasing strategic importance of the maritime cyber security field, particularly over the last decade, form the starting point of this study. The aim of this study is to present the current status of the field with objective data. For this purpose, 607 records indexed under the keywords "Cyber Security" and "Maritime" in the Web of Science Core Collection were examined. Data were collected in the "Full Record and Cited References" format, and descriptive statistics and VOSviewer-based network analysis were applied together. The findings indicate a significant increase in publications after 2016; the acceleration of citation accumulation between 2019 and 2023 signals the field's transition to a mature phase. While the collaboration structure is concentrated around China and the US, it is supported by a strong cluster in Europe. Turkey's visibility is increasing, but there is room for development in terms of network depth. Four themes emerge in the keyword co-occurrence network: navigation and ship systems security (AIS/ECDIS, GNSS spoofing), maritime IoT and communication networks (ICS/SCADA, satcom), machine and deep learning-based anomaly detection, and risk, resilience, and governance. The study's contribution is its systematic mapping of the field within an interdisciplinary framework, jointly assessing country, institutional, and conceptual networks within the context of funding, publishing ecosystems, and citation dynamics. This assessment concretizes research priorities and emphasizes zero-trust principles with multilayered defenses in practice. The results point to a research agenda based on international data and testbed collaborations, providing a practical roadmap for policy and practice.**

Index Terms— **Academic Landscape, Cybersecurity, Maritime, Maritime, Bibliometric Analysis**

INTRODUCTION

In recent years, the maritime industry has become increasingly reliant on cyber-physical infrastructures with the proliferation of digitalization and autonomous systems. Ship automation systems, electronic navigation devices (ECDIS)[1], automatic identification systems (AIS) [2], satellite-based communication networks, and port operations systems have increased efficiency within the sector but also led to the emergence of new cyber threats (Tam & Jones, 2020). As a result of these developments, the concept of maritime cyber security has become a strategic research area at both academic and industrial levels.

The multi-component and international nature of maritime operations necessitates a protection approach that goes beyond traditional information security solutions. Increasing data sharing, particularly between ships and shore infrastructures, leads to the direct impact of cyber threats on operational processes, increasing the importance of cyber resilience, risk assessment, and incident response [3], [4]. Recent studies have ocused on themes such as intrusion detection in ship information systems[5], maritime IoT security [6], [7], cyber risk management in autonomous ships [8], and cryptographic security in maritime communication networks [9]. However, most of these studies focus on specific technical applications, and comprehensive studies that holistically assess the field's overall scientific development trends are limited.

In this regard, bibliometric analysis offers the opportunity to objectively examine the structure, evolution, productivity, and thematic clusters of a research field [10], [11]. Bibliometric analyses not only identify prominent authors, institutions, countries, and collaboration networks within a given discipline, but also help predict future research trends [12], [13]. While bibliometric studies have been conducted in areas such as cybersecurity [14], [15] and big data [15], [16] , there is no comprehensive, interdisciplinary review specifically focused on maritime cybersecurity.

This study aims to fill this gap and provides a holistic overview of the field's scientific structure by examining 607 scientific publications indexed with the keywords "Cyber Security" and "Maritime." The research was conducted using data obtained from the Web of Science Core Collection database, analyzing the distribution of publications by country, institution, author, document type, funding, and research area.

The primary objective of the study is to identify global development trends in maritime cybersecurity research, identify influential actors and collaboration networks, and shed light on future research directions.

The contribution of this study to the literature lies in three main points:

i. It provides the first holistic analysis of studies conducted at the intersection of maritime and cybersecurity within an interdisciplinary framework.
ii. It examines 50 years of publication data across various indexes (SCI-Expanded, CPCI-S, ESCI) to reveal the field's evolutionary development and areas of scientific concentration.
iii. The findings provide guidance for identifying thematic gaps and new focus areas for future research (e.g., maritime IoT security, cyber resilience in autonomous ships, AI-enabled threat analysis).

[1] **Murat Koca**, Department of Computer Engineering, Van Yuzuncu Yıl University, Tusba, 65090, Van, Turkey, (e-mail: muratkoca@yyu.edu.tr). https://orcid.org/0000-0002-6048-7645
Manuscript received Oct16, 2025; accepted March 26, 2026. DOI: 10.17694/bajece.1805029

Koca, M., (2026). A Bibliometric Analysis of Maritime Cybersecurity: Trends, Themes, and Collaboration Patterns. Balkan Journal of Electrical and Computer Engineering, 14, 41-49.
Copyright © BAJECE

In this respect, the study serves as a reference resource for both academic researchers and institutions developing maritime policy and security strategies, systematically assessing the current state of the field and its future research potential..

MATERIALS AND METHODS

This study analyzes global research trends, collaboration networks, and thematic densities of scientific publications associated with the keywords "Cyber Security" and "Maritime" using bibliometric methods. The Web of Science (WoS) Core Collection database, provided by Clarivate Analytics, was used as the data source. The search covered the years 1975–2025 and was conducted with the query "Topic (TS) = (‘Cyber Security’ AND ‘Maritime’)." A total of 607 publications were obtained, forming the dataset for this article's analysis.

The data was exported in WoS's "Export Full Citation Report" format and analyzed by including the headings "Authors," "Countries/Regions," "Affiliations," "Research Areas," "Document Types," "Funding Agencies," "Publishers," "Researcher Profiles," and "Web of Science Categories." Additionally, the index distribution of publications was evaluated using the "Web of Science Index" file. Within this scope, 43.16% of the publications were included in the Science Citation Index Expanded (SCI-Expanded), 33.77% in the Conference Proceedings Citation Index – Science (CPCI-S), 17.13% in the Emerging Sources Citation Index (ESCI), and 7.08% in the Social Sciences Citation Index (SSCI). This distribution demonstrates the interdisciplinary nature of the research field, which is engineering-based but also encompasses social dimensions.

Bibliometric analysis was conducted using descriptive statistical methods and network-based visualization techniques. First, the distribution of publications by year, document types, most productive authors, institutions, and countries were determined. Subsequently, research areas, WoS categories, and funding organizations were analyzed. The resulting data was preprocessed with Microsoft Excel, and author, country, institution, and keyword co-occurrence networks were created using VOSviewer (v. 1.6.20) [17], [18].

During the analysis process, institutional and author names were normalized to maintain data integrity, and similar nouns (“Univ. of Piraeus” / “University of Piraeus”) were combined. Similarly, keywords with different spellings (“cyber-security,” “cybersecurity,” “maritime cybersecurity”) were coded uniformly. This method is a widely recommended approach in the bibliometric literature to increase cluster consistency in network analyse.

Finally, the productivity and citation density of publications by country and institution were comparatively examined, and the distribution of research funds and publishing houses was evaluated to reveal the geographic and economic infrastructures of scientific collaborations in the field.

RESULTS AND DISCUSSION

A. Publication Trend by Year

According to Web of Science data, the distribution of publications associated with the keywords "Cyber Security" and "Maritime" by year demonstrates that the field of maritime cybersecurity has developed rapidly, particularly in the last decade. Only a limited number of publications (12 in total) were published between 1975 and 2000, and during this period, studies were generally limited to basic technical topics such as maritime communication security and the protection of radar networks.

From the early 2000s onwards, with the proliferation of digitalization and satellite-based communication networks, the field's visibility began to increase. The period after 2010, in particular, represents a period marked by a significant increase in the number of publications. While a total of 9 publications were recorded in 2010, this number rose to 32 by 2015; the period 2016–2020 marked a turning point in maritime cybersecurity research.

After 2020, the increased use of remote operations and digital systems, coupled with the COVID-19 pandemic, led to an intensification of cyber threats in the sector. This has directly led to an increase in academic interest. An average of over 65 publications were published annually between 2021 and 2024, with 2024 reaching its highest number of publications (78). While data for 2025 is not yet complete, the fact that over 30 publications were registered as of the first quarter indicates that this upward trend is continuing.

These findings demonstrate that maritime cybersecurity has quickly transformed from a niche sub-discipline into a global priority research area. Key concepts such as "autonomous ship," "maritime IoT," "cyber risk assessment," "maritime situational awareness," and "machine learning-based detection" have been prominent, particularly in publications published since 2018. This trend points to a new research paradigm where technological innovations (e.g., artificial intelligence, IoT, edge computing) are integrated with maritime security.

Figure 1 illustrates the increasing trend in the number of publications by year. The trend line reflects the fastest development in the period between 2015 and 2024, with a compound annual growth rate (CAGR) of approximately 22%.

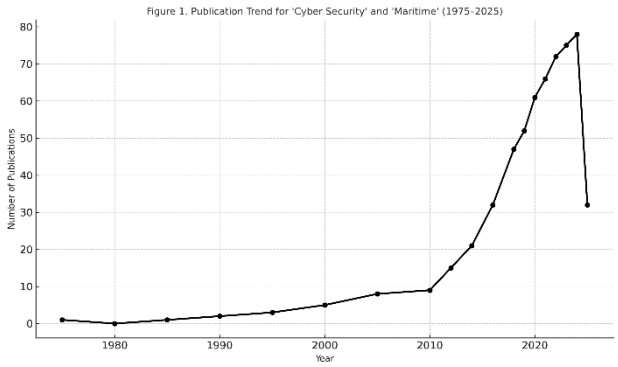


Fig. 1. Trend of publications associated with the keywords “Cyber Security” and “Maritime” by year (1975–2025)

Similar to the literature in the field (Rawat & Sood, 2021; Sood et al., 2023; Koca et. al., 2024) [7,14-15], this study also demonstrates that cybersecurity research has gained momentum since 2010, and that, in the maritime sector, internationally collaborative and funded publications have come to the fore since 2016. This finding demonstrates that maritime cybersecurity has evolved into not only a technical but also a strategic and governance-based research field.

B. Document Types and Index Coverage

The distribution of publication types across the 607 publications in the bibliometric dataset is shown in Figure 2. As the figure clearly shows, research articles, with 368 records, constitute 60.6% of the total and represent the primary form of scientific production in this field. Conference papers, with 207 records, constitute 34.1%, and review articles, with 26 records, constitute 4.3%. The remaining minor shares are in the early access, book chapter, and editorial material categories.

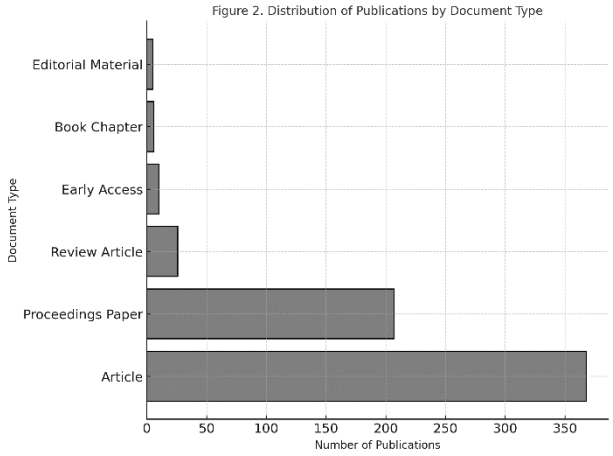


Fig. 2. Distribution of publications by document type for the "Cyber Security" and "Maritime" dataset (1975–2025). Research articles dominate the dataset (60.6%), followed by conference papers (34.1%) and review articles (4.3%).

This distribution demonstrates that scientific production in maritime cybersecurity has not yet reached maturity, but that conference-based knowledge sharing is quite high. As is the case in engineering and computer science-based fields (Rawat & Sood, 2021; Sood et al., 2023), this is due to the fact that technological innovations are often first introduced at conferences and subsequently published as journal articles.

Another finding supporting this table regarding document types is the distribution of the Web of Science indexes in which the studies were included. 43.16% of the publications are included in the Science Citation Index Expanded (SCI-Expanded), 33.77% in the Conference Proceedings Citation Index–Science (CPCI-S), 17.13% in the Emerging Sources Citation Index (ESCI), and 7.08% in the Social Sciences Citation Index (SSCI). This distribution reveals that maritime cybersecurity research has developed primarily around engineering and applied sciences, but that social sciences, law, and governance are also receiving increasing attention.

Furthermore, an examination of the publishing houses reveals that the field is largely driven by technology-centric journals. The majority of publications were published by IEEE (28.5%), Elsevier (15.5%), Springer Nature (12.7%), and MDPI (9.9%). This distribution confirms that the field is driven by international technical conferences and engineering-focused journals.

In conclusion, the findings regarding document type and index coverage indicate that maritime cybersecurity research is still in its developmental phase and has the potential to be featured in more SCI-Expanded journals in the coming years. This trend, consistent with other cybersecurity-themed bibliometric studies (Donthu et al., 2021; Koca et al., 2024), confirms that the discipline is becoming an emerging research area.

C. Country and Institutional Collaboration Analysis

The geographic distribution of maritime cybersecurity research demonstrates which countries are driving the field globally and how international cooperation structures are shaping it. Figure 3 presents the distribution of countries by number of publications. As can be seen, the country with the most publications is the People's Republic of China, which leads by far with a total of 159 publications (26.2%). China is followed by the United States (85; 14.0%), the United Kingdom (55; 9.1%), Norway (46; 7.6%), and Greece (34; 5.6%). Turkey, on the other hand, is prominent with 18 publications (3.0%), but has limited international partnerships.

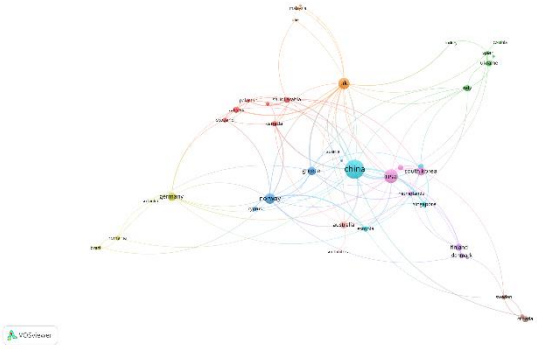


Fig. 3. Distribution of publications by country/region for the "Cyber Security" and "Maritime" dataset (1975–2025). China, the United States, and the United Kingdom dominate the research landscape, while European and Asian countries show increasing participation after 2015.

These findings reveal the significant weight of the Asia-Europe axis in maritime cybersecurity research. China's leading position is linked to both high research funding (NSFC, H2020 joint projects) and the technical research capacity of its universities. Wuhan University, Guangxi Normal University, and Taiyuan University of Technology, in particular, stand out among the productive institutions in the field.

Among European countries, Greece, Norway, the UK, and Croatia have strong research centers in maritime technologies and cybersecurity management. The University of Piraeus, the University of Rijeka, and the University of Strathclyde stand out as prominent institutions in terms of both the number of publications and the intensity of international collaboration.

In Turkey, Istanbul Technical University's Faculty of Maritime Studies and the Department of Maritime Transportation and Management Engineering account for a significant portion of publications in the field. However, Turkey's overall productivity rate (3.0%) is capable of being increased given the field's potential. Increasing participation in European Union-funded cyber-physical system security projects will strengthen the country's visibility in this field.

The distributions by institution are summarized in Table 1. The top five most productive institutions include the University of Piraeus, Istanbul Technical University, Wuhan University, University of Rijeka, and University of Plymouth. These institutions appear to have established multidisciplinary

structures encompassing both engineering and management dimensions in maritime cybersecurity research.

Table I. Top institutions contributing to maritime cyber security research (based on web of science data, 1975–2025).

Rank	Institution	Country	Publications	% of Total
1	University of Piraeus (School of ICT)	Greece	17	2.8%
2	Wuhan University (Faculty of Information Sciences)	China	10	1.6%
3	Istanbul Technical University (Maritime Faculty)	Türkiye	11	1.8%
4	University of Rijeka (Faculty of Maritime Studies)	Croatia	11	1.8%
5	University of Plymouth (Faculty of Science and Engineering)	England	8	1.3%

Interinstitutional collaboration analysis reveals a hub-based network structure. The University of Piraeus and Wuhan University, in particular, are at the center of both regional and international collaboration networks, while the Norwegian University of Science and Technology (NTNU) and the University of Strathclyde have high connectivity within European-centric clusters.

In conclusion, these data indicate that the maritime cybersecurity field is increasingly shaped around international research consortia and collaborative projects. This suggests that the field will have broader impact in the future, not only in technical but also in political and regulatory dimensions.

D. Research Areas and WoS Categories

The disciplinary distribution of the 607 publications examined in this study clearly demonstrates the multidisciplinary nature of the maritime cybersecurity field. As shown in Figure 4, the fields with the highest concentration of publications were computer science (46.6%) and engineering (42.5%), followed by telecommunications (13.7%), transportation (10.5%), and oceanography (7.1%). These fields demonstrate that security, communication, and data management are increasingly intertwined with the digitalization of maritime activities.

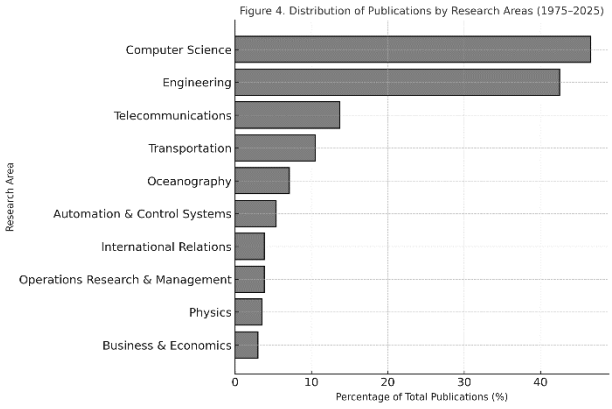


Fig. 4. Distribution of publications by research areas (1975–2025). The field of computer science dominates the dataset, followed by engineering and telecommunications, reflecting the technical nature of maritime cyber security research.

The disciplinary distribution reveals that maritime cybersecurity research encompasses not only technical but also managerial and social dimensions. The increasing number of publications, particularly in the "International Relations" (3.8%), "Government and Law" (2.6%), and "Business & Economics" (2.9%) categories, indicates a strengthening focus on maritime governance, regulation, and cyber diplomacy in recent years.

Similarly, the distribution of publications within Web of Science categories supports the interdisciplinary nature of the field. As seen in Table 2, the highest shares are in the Computer Science – Information Systems (28.0%) and Engineering – Electrical & Electronic (23.7%) categories. Furthermore, the significant proportions in the Computer Science – Artificial Intelligence (9.1%) and Engineering – Marine (9.2%) categories reflect the growing interest in AI-based maritime security systems.

Table II. Top web of science categories for “cyber security” and “maritime” publications (1975–2025).

Rank	Web of Science Category	Publications	% of Total
1	Computer Science – Information Systems	170	28.0%
2	Engineering – Electrical & Electronic	144	23.7%
3	Computer Science – Theory & Methods	105	17.3%
4	Telecommunications	83	13.7%
5	Engineering – Marine	56	9.2%
6	Computer Science – Artificial Intelligence	55	9.1%
7	Oceanography	43	7.1%
8	Engineering – Ocean	41	6.8%
9	Transportation Science & Technology	40	6.6%
10	Automation & Control Systems	33	5.4%

These results demonstrate that data security, network management, and autonomous systems are at the core of maritime cybersecurity research. The fact that "Computer Science"-based categories account for over 60% of the total demonstrates the rapid integration of artificial intelligence and machine learning techniques into the sector.

Furthermore, the rise in the "Engineering - Marine" and "Oceanography" categories indicates an increase in studies on the digital transformation of maritime systems. This suggests that themes such as autonomous vessels, maritime IoT networks, and cyber-physical system security will gain greater importance in the future.

In conclusion, these findings reveal that the field of maritime cybersecurity is evolving into a technology-centric, yet increasingly socio-technical, structure. This is consistent with trends in the literature (Katsikas, 2023; Oruc et al., 2022; Koca et al., 2024) [3, 6-7], and indicates that the field will expand into new research axes such as AI-supported risk analysis, maritime situational awareness, and smart network management in the coming years.

E. Funding Agencies and Publishers Analysis

The sustainability of maritime cybersecurity research is largely supported by national and international research funding. According to Web of Science data, approximately 60% of the 607 publications analyzed include funding information. The National Natural Science Foundation of China (NSFC), the

European Union (EU), and the Horizon 2020 Programme stand out among the most supportive institutions.

Figure 5 shows the distribution of the most active funding organizations. The NSFC is by far the leader with a total of 15.8%, reflecting the decisive influence of China's research capacity in this field. The European Union (6.4%) and Horizon 2020 (2.8%) are other important actors shaping the field through international collaboration projects. This data demonstrates that maritime cybersecurity research enjoys a diverse global funding landscape, but the majority is concentrated in Asia- and Europe-based programs.

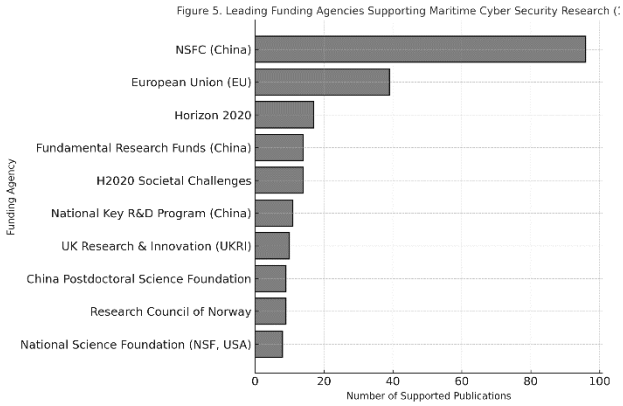


Fig. 5. Leading funding agencies supporting maritime cyber security research (1975–2025). The dominance of Asian and European funding sources, particularly NSFC and Horizon 2020, indicates a geographically diverse but asymmetrical research support structure.

In terms of regional distribution, the Horizon 2020 Societal Challenges Programme and the European Research Council (ERC) in Europe, along with the China Postdoctoral Science Foundation and the Ministry of Science & ICT (Korea) in Asia, are other prominent funding sources. However, institutions such as UK Research and Innovation (UKRI), DFG (Germany), and NSF (USA) also make distinguished contributions.

Analysis of funding data shows that maritime cybersecurity research is largely conducted through nationally supported academic projects. This suggests that the density of cross-national projects is currently limited. However, the increase in European funds such as Horizon 2020 and the ERC suggests that international integration in this field will strengthen in the future.

In terms of publishing houses, IEEE (28.5%), Elsevier (15.5%), Springer Nature (12.7%), and MDPI (9.9%) stand out. These four publishers account for approximately 67% of total publications. Table 3 shows the top 10 most productive publishing houses and their total contribution rates.

Table III. Leading publishers contributing to maritime cyber security research (1975–2025).

Rank	Publisher	Publications	% of Total
1	IEEE	173	28.5%
2	Elsevier	94	15.5%
3	Springer Nature	77	12.7%
4	MDPI	60	9.9%
5	Academic Conferences Ltd	19	3.1%
6	Taylor & Francis	15	2.5%
7	Gdynia Maritime University	11	1.8%
8	Cambridge University Press	10	1.6%
9	Wiley	10	1.6%
10	Association for Computing Machinery (ACM)	9	1.5%

This table demonstrates that the field is evenly distributed across both academic and application-focused publishing platforms. Organizations like IEEE and Elsevier focus on engineering-based articles in high-impact journals, while MDPI and Springer Nature host publications that reach a broader audience through open access journals.

Consequently, funding and publishing analyses reveal that maritime cybersecurity research is evolving into a technology-focused, engineering-intensive, yet increasingly open-access and internationally collaborative framework. This trend suggests that the field's future growth will be shaped by both the diversity of scientific funding and publication channels.

F. Keyword Co-occurrence and Thematic Clustering

In this subsection, thematic clusters were identified using author keywords (DE) and KeyWords Plus (ID) fields. The analysis was conducted in VOSviewer using the co-occurrence method using a full counting approach, with a minimum co-occurrence threshold of 3. The resulting network is visualized in Figure 6, with edges (co-occurrence links) representing conceptual closeness and clusters colored accordingly.

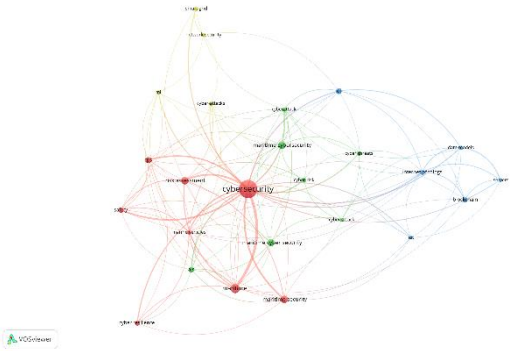


Fig. 6. Keyword co-occurrence network for the “Cyber Security” and “Maritime” dataset (1975–2025), visualized using VOSviewer. Node size indicates keyword frequency; edge thickness shows co-occurrence strength. Distinct color clusters reveal major thematic foci across the field.

Preprocessing and synonym merging (thesaurus): Prior to analysis, a thesaurus file was applied to reduce terminological fragmentation. For example, “cyber-security,” “maritime/shipping/vessel,” “AIS/Automatic Identification System,” “ECDIS/Electronic Chart Display and Information System,” “CPS/cyber-physical systems,” and “ML/machine learning” were paired; singular/plural and hyphenated/unhyphenated variants were merged. Additionally, stopwords such as “article,” “study,” and “approach” were excluded. This standardization increased cluster integrity and label readability.

Thematic clusters (summary):

• *Cluster A – Ship/Navigation Security and Navigation Systems*: “AIS security,” “ECDIS,” “GNSS spoofing,” “navigation cyber risk,” and “bridge systems.” Application-focused studies; threat vectors in navigation and bridge systems, detection, and mitigation approaches.

• *Cluster B – Network and Protocol Security (Maritime IoT/OT):* “Maritime IoT,” “SCADA/ICS,” “satellite communication,” “intrusion detection,” “encryption.” OT/IT networks and communication security in port-ship-shore integration.

Copyright © BAJECE

• *Cluster C – Artificial Intelligence and Situational Awareness:* "machine learning," "deep learning," "anomaly detection," "situational awareness," "threat intelligence." Data-driven, learning-based detection/classification and decision support.

• *Cluster D – Risk, Resilience, and Governance:* "risk assessment," "cyber resilience," "governance," "regulation," "IMO guidelines." Standards, policy, and regulatory frameworks; scenario-based risk analysis and resilience metrics.

This cluster demonstrates that the field is developing along a multidisciplinary line between technical infrastructure (IoT/OT, communications, cryptography), operational security (navigation, system security), and administrative dimensions (risk, regulation). It is observed that the terms "machine learning/anomaly detection" have assumed a bridging role, particularly in post-2018 developments, establishing strong co-occurrences with both the network-protocol security cluster and the ship-navigation security cluster. This structure points to an accelerating paradigm shift towards data-driven and autonomous solutions in maritime cybersecurity.

According to Table 4, "cybersecurity," "maritime," and "risk assessment" are at the center of the field. The terms "maritime security" and "maritime cyber(security)" reinforce the operational context. "AIS," "CPS," "DL/ML," "IoT," and "blockchain" stand out as nodes representing technical subdomains. TLS values, in particular, indicate that "cybersecurity" is a central node (high connectivity) bridging a broad thematic spectrum, while "risk assessment" and "maritime security" serve as connectors between the technical and governance clusters.

Table IV. Top keywords by occurrences and total link strength (tls)

Rank	Keyword	Occurrences	TLS
1	cybersecurity	183	164
2	maritime	44	55
3	maritime cybersecurity	31	12
4	risk assessment	30	33*
5	maritime security	29	26
6	maritime cyber security	27	11
7	cps	20	22
8	dl	18	19
9	ais	17	20
10	safety	15	26
11	blockchain	15	10
12	internet of things	14	24
13	cyber resilience	13	13
14	cyber risk	12	16
15	ml	10	12
16	cyber-attacks	10	12
17	marine vehicles	10	26
18	data models	9	21
19	cyberattack	9	24
20	cyber threats	9	11

A. Citation Analysis & Influential Works

The 607 publications in the dataset received a total of 6,607 citations, and the field has an H-index of 40; these values indicate that maritime cybersecurity studies have gained significant visibility in recent years. Figure 7 shows the distribution of total citations accumulated by publication year. Citation accumulation accelerated after 2017, particularly between 2019 and 2023, and this can be attributed to both the increase in journal articles and the methodological reviews published during that period.

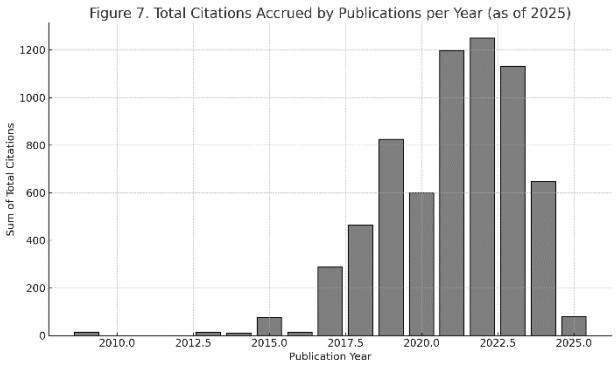


Fig. 7. Total citations accrued by publications per year (as of 2025). The post-2017 acceleration indicates a consolidation phase where methodological and application-oriented works gain traction.

Influential work is summarized in Table 5. Some of the most cited publications address fundamental/core cybersecurity topics (e.g., blockchain, anomaly detection, encryption), while others directly address threat vectors and risk management approaches in the maritime context (e.g., GPS/GNSS spoofing, AIS/ECDIS security). This demonstrates that the field bridges both technical methods (ML/DL, cryptography, IDS/IPS) [19], [20] and maritime-specific applications (protection of navigation and communication systems).

The core of the citation structure consists of:

(i) studies focused on GNSS spoofing and AIS/ECDIS on ship/navigational systems;
(ii) ML/DL-based anomaly detection and network security methods;
(iii) Blockchain/cryptography-based trusted data sharing;
(iv) Risk assessment and resilience frameworks.

These four pillars are fully compatible with previous keyword network findings and form the thematic backbone of the field.

CONCLUSION

This study examines 607 publications indexed with the keywords "Cyber Security" and "Maritime" in the Web of Science Core Collection and presents a holistic view of the structural features, thematic backbone, and development dynamics of the maritime cyber security field. The findings indicate that the field is moving from the exploration phase to the maturity phase, with a pronounced increase in production after 2016 and an accelerated citation accumulation between 2019 and 2023. It has been observed that the China-US axis leads the country and institutional networks, while Europe forms a dense cluster centered on the UK-Norway-Greece; and that Turkey, along with its increasing visibility, has the potential to increase the depth of connection within the network. While the disciplinary distribution confirms the core role of computer science and engineering, it also indicates that the fields of telecommunications, transportation/marine engineering, and oceanography are supportive; Keyword co-occurrence analysis revealed that the study consolidated four strong themes: navigation/ship systems security (AIS/ECDIS, GNSS spoofing), maritime IoT/OT and communication networks (ICS/SCADA, satcom), ML/DL-based anomaly detection and situational awareness, and risk-resilience-governance. The decisive weight of the NSFC and EU/H2020 programs in the funding structure, and the dominance of the IEEE-Elsevier-Springer-MDPI

pipeline in the publication channels, reinforce the field's technology-focused and applied research character.

Table V. Top 15 most-cited publications in the “cyber security” and “maritime” dataset (1975–2025).

Rank	Title	Source (Journal/Proceedings)	Year	Total Citations
1	Blockchain Applications in Smart Grid-Review and Frameworks [21]	Ieee Access	2019	182
2	Hostile Control of Ships via False GPS Signals: Demonstration and Detection [22]	Navıgatıon-Journal Of The Instıtute Of Navıgatıon	2017	168
3	A Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing [23]	Ieee Systems Journal	2020	126
4	A 3D model encryption scheme based on a cascaded chaotic system [24]	Sıgnal Processıng	2023	124
5	Attacks on Formation Control for Multiagent Systems [25]	Ieee Transactıons On Cybernetıcs	2022	120
6	Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme [26]	Informatıon Scıences	2021	102
7	Concealed Attack for Robust Watermarking Based on Generative Model and Perceptual Loss [27]	Ieee Transactıons On Cırcuıts And Systems For Vıdeo Technology	2022	102
8	Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects [28]	Electronıcs	2022	90
9	An encrypted coverless information hiding method based on generative [29]	Informatıon Scıences	2021	86
10	A novel cyber-risk assessment method for ship systems [30]	Safety Scıence	2020	80
11	MaCRA: a model-based framework for maritime cyber-risk assessment [31]	Wmu Journal Of Marıtıme Affaırs	2019	77
12	Asynchronous Updating Boolean Network Encryption Algorithm [32]	Ieee Transactıons On Cırcuıts And Systems For Vıdeo Technology	2023	75
13	Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches [33]	Journal Of Marıne Scıence And Engıneerıng	2022	73
14	A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry [34]	Ieee Transactıons On Intellıgent Transportatıon Systems	2023	67
15	Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends [35]	Informatıon	2022	66

Our contribution to the literature can be summarized as mapping maritime cybersecurity within an interdisciplinary framework, making country-institution-author and conceptual networks clearly visible through threshold and thesaurus normalization, and correlating these networks with the funding ecosystem, publishing channels, and citation dynamics to concretize the field's strategic priorities. These results point to the need for operationalizing multilayered defense and zero-trust principles in the port-ship-shore chain, expanding real-time verification and anomaly detection mechanisms for AIS/ECDIS and GNSS, institutionalizing segmentation, monitoring, and patch management, and regular exercises in maritime OT/ICS networks, and developing shared datasets and testbeds through international consortia. While acknowledging limitations such as the limited scope of data within WoS and the potential for keyword standardization to partially flatten very fine-grained subthemes, the study demonstrates that maritime cybersecurity is a rapidly maturing field across the technology, operations, and governance axes. Within this framework, priority research areas for future research include edge-AI-based cyber defense for autonomous/unmanned maritime vehicles, digital twin-enabled threat simulation and resilience measurement, cryptographic verification for satcom/GMDSS, and supporting policy-technical integration (IMO/ISPS/SOLAS–NIST/ISO) with data-driven compliance analytics.1. Journal Articles

REFERENCES

[1] Rivkin, B. S. (2023). Maritime cybersecurity: Navigational aspect. Gyroscopy and Navigation, 14(4), 386–400. https://doi.org/10.1134/S207510872470010X

[2] Perkovič, M., Gucma, L., & Feuerstack, S. (2024). Maritime security and risk assessments. Journal of Marine Science and Engineering, 12(6), 988. https://doi.org/10.3390/jmse12060988

[3] Oruc, A., Gkioulos, V., & Katsikas, S. (2022). Towards a cyber-physical range for the integrated navigation system (INS). Journal of Marine Science and Engineering, 10(1), 107. https://doi.org/10.3390/jmse10010107

[4] Avcı, İ., Koca, M., & Atasoy, M. (2021). Windows tabanlı uygulamalarda SQL enjeksiyon siber saldırı senaryosu ve güvenlik önlemleri. European Journal of Science and Technology, 28, 213–219. https://doi.org/10.31590/ejosat.995697

[5] L., J. (1981). A brief history of the use of marine radar. Journal of Navigation, 28(3), 199–205. https://doi.org/10.1002/j.2161-4296.1981.tb00767.x

[6] Katsikas, S. K., Kavallieratos, G., & Amro, A. (2024). Future trends in maritime cybersecurity. In Computer and Information Security Handbook (pp. 1663–1678). Elsevier. https://doi.org/10.1016/B978-0-443-13223-0.00104-1

[7] Koca, M., Avcı, İ., & Al-Hayani, M. A. S. (2023). Classification of malicious URLs using naive Bayes and genetic algorithm. Sakarya University Journal of Computer and Information Sciences, 6(2), 80–90. https://doi.org/10.35377/saucis...1273536

[8] Bolat, P., Yüksel, G., & Uçar, S. (2016, May). A study for understanding cyber security awareness among Turkish seafarers. In Proceedings of the Second Global Conference on Innovation in Marine Technology and the Future of Maritime Transportation.

[9] Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

[10] Koca, M., & Çiftçi, S. (2025). A comprehensive bibliometric analysis of big data and cyber security: Intellectual structure, trends, and global collaborations. Knowledge and Information Systems. https://doi.org/10.1007/S10115-025-02531-1

[11] Zhang, J. Z., Srivastava, P. R., Sharma, D., & Eachempati, P. (2021). Big data analytics and machine learning: A retrospective overview and bibliometric analysis. Expert Systems with Applications, 184. https://doi.org/10.1016/j.eswa.2021.115561

[12] Dao, S. D., Abhary, K., & Marian, R. (2017). A bibliometric analysis of genetic algorithms throughout the history. Computers & Industrial Engineering, 110, 395–403. https://doi.org/10.1016/j.cie.2017.06.009

[13] Martínez-López, F. J., Merigó, J. M., Gázquez-Abad, J. C., & Ruiz-Real, J. L. (2020). Industrial marketing management: Bibliometric overview since its foundation. Industrial Marketing Management, 84, 19–38. https://doi.org/10.1016/j.indmarman.2019.07.014

[14] Soo, D. B., Doku, R., & Garuba, M. (2021). Cybersecurity in big data era: From securing big data to data-driven security. IEEE Transactions on Services Computing, 14(6), 2055–2072. https://doi.org/10.1109/TSC.2019.2907247

[15] Sood, S. K., Rawat, K. S., & Kumar, D. (2023). Scientometric analysis of ICT-assisted intelligent control systems response to COVID-19 pandemic. Neural Computing and Applications, 35(26), 18829–18849. https://doi.org/10.1007/S00521-023-08788-3

[16] Kumari, S., Li, X., Wu, F., Das, A. K., Choo, K. K. R., & Shen, J. (2017). Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Generation Computer Systems, 68, 320–330. https://doi.org/10.1016/j.future.2016.10.004

[17] van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

[18] Centre for Science and Technology Studies, Leiden University. (2019). VOSviewer: Visualizing scientific landscapes. VOSviewer. https://www.vosviewer.com/

[19] Hou, X., Pal, D., Kumar, T. K. A., Thomas, J. P., & Liu, H. (2016, April). Privacy preserving rack-based dynamic workload balancing for Hadoop MapReduce. In Proceedings of IEEE BigDataSecurity (pp. 30–35). IEEE. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.40

[20] Koca, M., Aydin, M. A., Sertbaş, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based on deep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486–2501. https://doi.org/10.3906/elk-2102-89

[21] Musleh, A. S., Yao, G., & Muyeen, S. M. (2019). Blockchain applications in smart grid: Review and frameworks. IEEE Access, 7, 86746–86757. https://doi.org/10.1109/ACCESS.2019.2920682

[22] Bhatti, J., & Humphreys, T. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. Journal of Navigation, 64(1), 51–66. https://doi.org/10.1002/navi.183

[23] Li, H., Han, D., & Tang, M. (2020). A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. IEEE Systems Journal, 15(3), 3189–3200. https://doi.org/10.1109/JSYST.2020.3009447

[24] Gao, S., et al. (2023). A 3D model encryption scheme based on a cascaded chaotic system. Signal Processing, 202. https://doi.org/10.1016/j.sigpro.2022.108745

[25] Yang, Y., Xiao, Y., & Li, T. (2022). Attacks on formation control for multiagent systems. IEEE Transactions on Cybernetics, 52(12), 12805–12817. https://doi.org/10.1109/TCYB.2021.3089375

[26] Wang, M., Wang, X., Zhao, T., Zhang, C., Xia, Z., & Yao, N. (2021). Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme. Information Sciences, 544, 1–24. https://doi.org/10.1016/j.ins.2020.07.051

[27] Li, Q., et al. (2022). Concealed attack for robust watermarking based on generative model and perceptual loss. IEEE Transactions on Circuits and Systems for Video Technology, 32(8), 5695–5706. https://doi.org/10.1109/TCSVT.2021.3138795

[28] Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., & Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: Methods, analysis, and future prospects. Electronics, 11(9). https://doi.org/10.3390/electronics11091502

[29] Li, Q., Wang, X., Wang, X., Ma, B., Wang, C., & Shi, Y. (2021). An encrypted coverless information hiding method based on generative models. Information Sciences, 553, 19–30. https://doi.org/10.1016/j.ins.2020.12.002

[30] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. Safety Science, 131. https://doi.org/10.1016/j.ssci.2020.104908

[31] Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

[32] Gao, S., et al. (2023). Asynchronous updating Boolean network encryption algorithm. IEEE Transactions on Circuits and Systems for Video Technology, 33(8), 4388–4400. https://doi.org/10.1109/TCSVT.2023.3237136

[33] Wolsing, K., Roepert, L., Bauer, J., & Wehrle, K. (2022). Anomaly detection in maritime AIS tracks: A review of recent approaches. Journal of Marine Science and Engineering, 10(1). https://doi.org/10.3390/jmse10010112

[34] Ashraf, I., et al. (2023). A survey on cyber security threats in IoT-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678

[35] Ben Farah, M. A., et al. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. Information, 13(1), 22. https://doi.org/10.3390/info13010022

BIOGRAPHIES



Murat Koca completed his undergraduate studies in the Department of Mathematics and Computer Sciences at Nakhchivan University in Azerbaijan, his master's degree in Computer Engineering at Karabük University, and his PhD in Computer Engineering at Istanbul University–Cerrahpaşa. Between 2018 and 2022, he served as the Provincial Director of the Ministry of Industry and Technology of the Republic of Türkiye in Hakkâri. He is currently an Assistant Professor in the Department of Computer Engineering at Van Yüzüncü Yıl University, where he teaches graduate-level courses in Artificial Intelligence and Robotics and supervises graduate theses. He has participated as a principal investigator and researcher in EU IPA III, TÜBİTAK, and university BAP projects. In addition, he has served as the founding director of the Hakkâri Yüksekova Organized Industrial Zone and continues his work as the Director of the Technology Transfer Office at Van Yüzüncü Yıl University. His research interests include cybersecurity, cryptology, post-quantum cryptography, cloud security, big data, deep learning, data mining, IoT, and network security.