

Cyber Threat Intelligence for Hospitals a A Systematic Literature Review

Benedikt Michaelis

`benedikt.michaelis@th-brandenburg.de`

Brandenburg University of Applied Sciences <https://orcid.org/0009-0009-8233-8454>

Carina Schwabe

Brandenburg University of Applied Sciences <https://orcid.org/0009-0009-7769-4518>

Stefan Stein

Brandenburg University of Applied Sciences <https://orcid.org/0000-0001-7403-1158>

Michael Pilgermann

Brandenburg University of Applied Sciences <https://orcid.org/0000-0002-1129-437X>

Systematic Review

Keywords: Cyber Threat Intelligence (CTI), cybersecurity, healthcare, hospitals, Literature Review, Medical Cyber Physical Systems (MCPS)

Posted Date: September 21st, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10457606/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Cyber Threat Intelligence for Hospitals ^a

A Systematic Literature Review

Benedikt Michaelis^{b,1,2}, Carina Schwabe^{c,1,2}, Stefan Stein^{d,1}, Michael Pilgermann^{e,1}

¹Department of Computer Science and Media, Brandenburg University of Applied Sciences, Magdeburger Straße 50, 14770 Brandenburg an der Havel, Germany

²Department of Mathematics and Computer Science, Freie Universität Berlin, Arnimallee 14, 14195 Berlin

Abstract Hospitals provide indispensable services to individuals and society. The urgent need for continuous service and the high value connected with the associated data make them attractive targets for cyberattacks. Consequently, lives depend on sufficient cybersecurity measures. Cyber Threat Intelligence allows hospitals to implement proactive strategies and measures, and is therefore recommended in research on cybersecurity for hospitals. This article examines research findings in the field of Cyber Threat Intelligence specifically for hospitals and correlates the findings with generic findings regarding issues and proposed solutions. Despite the criticality of hospital operations and a currently insufficient preparation against cyberattacks, research specifically on Cyber Threat Intelligence for hospitals is limited. The review identified seven publications. The research examined is characterized by investigations on the collection and processing of intelligence as well as suitable sharing. The problems described in generic research are also present here. This includes the persisting discussions on CTI and key terminology as well as a missing organizational perspective. Consequently, the article proposes a short definition of key terminology related to CTI and proposes the leading factors for research specifically for hospitals. This includes that presented solutions must match an acceptance level under practitioners and match requirements of data protection and cyber security. In addition, medical devices as a common source of intelligence have to be thoroughly researched, as well as the implementation

of sharing networks that incorporate adjacent organizations like emergency services and medical offices.

1 Introduction

Advances in medicine are a factor that contributes, among others, to a doubled life expectancy in Germany since the 19th century [1]. Improvements in medical care have been accompanied by technological advances in medicine. From monitoring vital signs to electronic implants and robots that assist in surgery, the daily routines of patients and medical professionals are versatily characterized by technical devices [2]. The essential services that hospitals provide for both individuals and society demand the mandatory requirement to protect them from attacks. The attacks themselves may cause malfunctions or failures that can cost lives and cause financial damage. In addition, the ruling of hospitals as critical infrastructure in different states, such as Germany [3] and the United States of America [4] honors the importance of hospitals. It is inherently clear that medical systems must function flawlessly. Every single case of patient outcomes that are negatively influenced by failing technical systems is one case too many. The observed lack of protection against cyberthreats in hospitals [5] urges the need to strengthen the protection strategies used.

Therefore, efforts to protect hospitals from cyberattacks are vital in an emerging area of attacks against hospitals. According to the European Network and Information Security Agency (ENISA), healthcare is the third largest sector targeted by ransomware attacks in the European Union (EU) [6]. This totals to 309 reported incidents affecting cybersecurity in the health sector in the EU in 2023 [7] and 389 successful ran-

^aThis work was funded by Brandenburg University of Applied Sciences.

^be-mail: benedikt.michaelis@th-brandenburg.de

^ce-mail: carina.schwabe@th-brandenburg.de

^de-mail: stefan.stein@th-brandenburg.de

^ee-mail: michael.pilgermann@th-brandenburg.de

somware hits on healthcare institutions in the US in 2024 [8].

Protecting data, devices, and associated functionalities is a challenge for hospitals. It is as important to hospitals for reasons of patient safety as it is for financial reasons [9]. To counteract these emerging threats, suitable measures must be established. Implementing Cyber Threat Intelligence (CTI) as a proactive measure is considered in different researches as a suitable measure for hospitals as a subset of critical infrastructures or for critical infrastructures themselves [10–13]. CTI can help implement targeted defensive measures, rather than indiscriminately hardening an organization. This can assist, in particular, counteracting attacks based on otherwise unknown vulnerabilities. Additionally, this can save rare resources due to the targeted deployment of human and financial resources based on intelligence. To assess whether the maturity of hospital specific CTI research matches the proposed need of CTI as a measure for hospitals (according to the aforementioned studies) a systematic literature review was conducted. Additionally, the review aims to compare the problems and research directions from general CTI research with hospital specific research and to carve out specific properties that come with applying CTI in a hospital context.

To improve future research, the following sections will introduce the topic with information on CTI, the current state of research for hospitals, resulting problems, and proposed future research directions. Section 2 introduces fundamental terminology and concepts, including the current state of research on CTI, including different levels of abstraction of research. It summarizes findings on key terminology and technical aspects of CTI. Section 3 introduces the methodology guiding the systematic search and review of CTI research in hospitals over a period of 2020 to May 2025. First, the section presents the research questions that guide the research in Subsection 3.1 and then the conducted steps for the collection of 1,966 search results, the screening of these results, the data extraction applied to the remaining 7 publications and statements on the quality assessment in subsections 3.2 to 3.5. The extracted information is presented in section 4 to answer each of the research questions presented in the subsections 4.1 to 4.6. The findings gained are utilized in a discussion (see Fig. : a definition is proposed and applied to the examined literature, and future research directions are given in the following section 5, followed by a summary in the final section 6.

2 Related Work

Protecting values and assets in an organization by a proactive strategy that utilizes information about potential threats (intelligence) is the main idea of CTI. It is therefore a subdomain of cybersecurity. Furthermore it aggregates knowledge from different sources to gain intelligence about attackers, motives, tactics, and techniques. The intelligence gained is delegated to different recipients or can be used as input for different counter measures such as anomaly detection or incident response. CTI has a variety of published research articles and can assist hospitals in protecting their vital assets effectively. While targeted measures resulting from implementing CTI can save financial or human resources, the implementation and realization of CTI may come with an overhead of financial and human resources. This necessary effort may deter hospitals from implementing CTI, praising research on tailored solutions that reduce the costs for hospitals.

The first structured search could not identify research that systematically reviewed the current state of research on CTI specific for hospitals. In addition, hospitals have probably not broadly adapted to CTI. Only less than half of the participants of a study for the German Hospital Federation provided information on CTI sources [14]. This may be contingent upon the highly likable need for a special approach. For example Koster pointed out the special requirements that come with medical devices [15]. Digital medical devices can occur in different shapes and be described with different terminology. Medical devices can be for example stationary, mobile, externally worn by a patient, or be an implant. Terminology and concepts can overlap, as stated by Weber et al. [16]. Terminology like Internet of medical Things (IoMT), Medical Cyber Physical Systems (MCPS), or Remote Patient Monitoring Systems (RPMs) can all inherit (digital) medical devices that can be related to hospitals as they send, provide or receive data from or for hospitals. Additionally, they can be located in a hospital.

Despite the limited amount of research on CTI for hospitals mentioned above, CTI has a variety of published reviews on different aspects and solutions and is widely considered in different research [17]. Aminu et al. noted that CTI should be used for situational awareness and to realize active defense [11]. It can harden and optimize established practices [12] and the sharing of CTI is key. CTI sharing strengthens individual security [10] because a single organization does not have an exhaustive view of the problem space [18]. The sharing of CTI is counteracted by often unconsidered supply chains [19]. In addition, many threat alerts do not

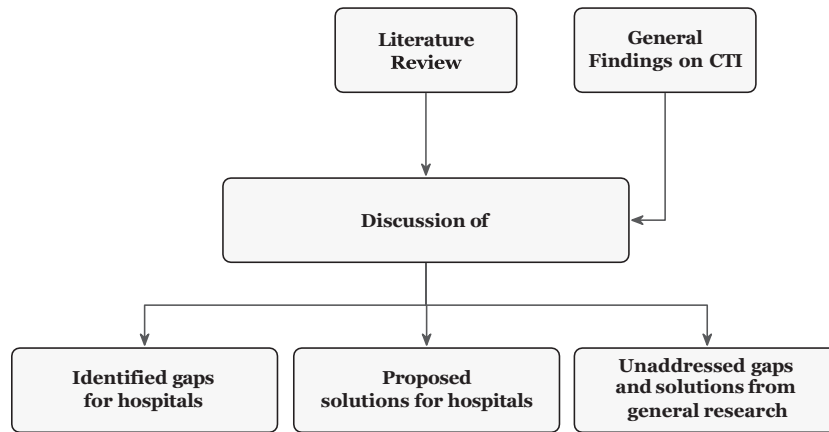


Fig. 1 Main Paper structure with focus on discussion. Structure of literature review is presented in section 3

claim any effect. There is a need to present intelligence in a way that allows users to see and understand alerts [20]. This is more difficult to establish considering the growth in the volume of data that must be collected and analyzed [21]. Collective adherence to sharing would benefit all, but is still perceived as a competitive disadvantage according to Jesus et al. [22] and Ainslie et al. [21] or is prevented by conflicts with organizational policy, regulation and law, and fear of losing intellectual property [21]. For hospitals data privacy may be a reason that fits better than competitive reasons. In particular, when sharing CTI in hospitals, pseudonymization and anonymization of data should be considered to prevent the disclosure of sensitive data, as stated by Rajamäki et al. [23]. They also discussed the need to check compliance with the General Data Protection Regulation (GDPR) and Network and Information Systems Directive (NIS2) of the European Union and to ensure data protection and critical infrastructure security, especially when CTI is planned to be shared. Sharing and handling CTI from the perspective of NIS2 and GDPR probably holds hospitals back. Additional obstacles include diverse implementations of sharing standards, establishing trust, and financial barriers [21]. This adds to the observation of Riesco et al. that organizations in general need motivation to share CTI with their peers [24].

The vital role that sharing plays is also represented by the variety of sharing and data standards with different strengths and weaknesses. Wagner et al. list popular standards for the sharing and description of intelligence [17]. They named the Structured Threat Information Expression (STIX), Trusted Automated eXchange of Indicator Information (TAXII), Open Threat Partner Exchange (OpenTPX) and Malware Attribute Enumeration and Characterization (MAEC) among others. A more detailed presentation is provided by Mavroei-

dis and Bromander [25]. They distinguish between taxonomies, sharing standards, and ontologies. As sharing standards, they include STIX, MAEC, and Open Indicators Of Compromise (OpenIOC). Nine taxonomies were listed. This includes, among others, Common Vulnerabilities and Exposures (CVE), the National Vulnerability Database (NVD), Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), the Common Vulnerability- and the Common Weakness Scoring System (CVSS, CWSS). In addition, they include 13 ontologies, such as the Unified Cyber Ontology (UCO) or STUCCO. A list of CTI-related standards is also provided by Sakellariou et al. [26] who name STIX, TAXI, CVE, ATT&CK, and OpenIOC, among others. There is a critical risk of disclosing information that is correlated with the standards [22]. Jesus et al. concluded that the risk of disclosing confidential information differs according to the standard implemented. Moreover, Wagner et al. [17] noted that CTI indicators neglect the Internet of Things (IoT) and Industrial Internet of Things (IIoT) and mainly focus on enterprise Information Technology (IT). Finally, Santos et al. deem the adoption of standardized frameworks essential as a basis for the integration of tools in and secure sharing between organizations [27]. In addition, they concluded that CTI solutions should be specifically designed for digital environments (including IoT and 5G networks).

Data transformed into intelligence can originate from different types of sources. Rahman et al. evaluated the sources used for CTI mining in 38 studies and detected threat reports as the most common source, with 39% of the publications exploring them [28]. Also common sources were forums (28%), Twitter (21%), and blogs (11%). Version control repositories, system and application logs, and darknet marketplaces were all part of one research (2%). Provenance remains a fundamental and contentious problem in the interpretation of intelli-

gence. This includes assessing authenticity, originality, and trustworthiness [21].

Finally, despite the large amount of research published on CTI, the perspective of organizational practice is still largely absent, according to Ainslie et al. [21]. They reason that this is due to the missing access for researchers to sensitive cyber practices and processes from organizations and the absence of social scientists in the field who could guide with the necessary methodology. Additionally, they propose that researchers should distinguish between praxis (what practitioners do) and practice (what practitioners are supposed to do through policy and training) [21]. Although the organizational perspective is underrepresented in research, some specifics should already be considered in the context of hospitals and healthcare. Standards for medical device certification, clinical safety constraints, SOC workflows and change management in hospitals, as well as legacy systems, limited funding options, or regulations (e.g. Health Insurance Portability and Accountability Act in the US) define hospital environments.

Platforms are essential for the implementation of CTI in practice. Irfan et al. [29] identify three components present in the research on CTI. These are a data collection component, a data analysis component, and an information platform. The components are equally relevant, but the de facto component is an information platform for sharing and dissemination. In addition, they describe a supplementary hurdle for practice: no CTI framework is considered applicable for all, as each organization is unique. Although organization is named by Irfan et al. domain or sector will probably be more suitable. The changing requirements for CTI frameworks emphasize the need for a unique solution that supports hospitals with their specific needs.

Despite extensive research on CTI, there are basic discrepancies in the interpretation of Cyber Threat Intelligence. Mavroeidis and Bromander [25] argued that *"vaguely defined terminology leads to confusion among experts [...]"* in 2017 and Sakellariou et al. [26] stated five years later in 2022 that *"the lack of precise definitions of key concepts of CTI leads in many cases to misunderstanding and confusion when authors use different terms for the same concept."* Different publications have proposed concepts, terms, and definitions. Some of these are introduced below.

The term (Cyber Threat) Intelligence has traditionally originated in military intelligence studies [21]. The United States Army defines CTI as: *"(1) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or*

potential operations and (2) the activities that result in the product; and (3) the organizations engaged in such activities." [30]. Similarly, Lowenthal proposed to encompass three perspectives: a view as a process, a product, and an organization [31]. Research conceptualizes and discusses CTI primarily as a technology, data or information, or a technical challenge [21]. Those three fields could indirectly be aligned with the original definition. Data and information can be aligned with the product. Although similarities are visible, it is not as clear and direct to align the remaining focuses: technology with organization and technical challenge with activities/processes. In addition, an organization includes staff or people associated with the work, as well as a process that incorporates people and is not only dependent on technical considerations.

However, CTI is inherently dependent on technology and its associated concepts. Chismon and Ruks [32] presented a concept to categorize CTI into subtypes classified in two dimensions: time period of use and level of abstraction. This allows intelligence to be categorized into strategic, tactical, operational, and technical subtypes as stated in Table 1. Each subtype serves different target groups; for example, technical intelligence with a low abstraction level and short time use is ideal for staff in a Security Operations Center (SOC) or an Incident Response (IR) team. Building on this, a detailed concept is provided by Sakellariou et al. [26] who present the subtypes of Chismon and Ruks as CTI Intelligence Views. In addition, they present the CTI Frame of Reference and CTI Complexity Factors (information sharing, security operations, big data, representation, quality of intelligence), leading to their presentation of a Cyber Threat Intelligence Reference Model.

3 Methodology

Although CTI is often listed as an essential strategy for protecting critical infrastructure, such as hospitals [10–13], initial searches suggest that the results for this field of research are limited and the research and level of application of CTI do not match the proposed application. Therefore, for this study a systematic review of the currently available, recent research was conducted to ensure that future research can build on the currently available findings and to bring together parallel research that may exist, for example due to unknown or unconsciously used synonymous terminologies. Additionally, this review aimed to reflect existing research on existing research directions and detected problems for CTI in general. It aimed at detecting specifics for CTI applied in or conceptualized for hospitals. The goals of

Table 1 Subtypes (*italic*) of threat intelligence including how they are characterized and target audiences (gray) based on a figure by Chismon and Ruks [?]

<i>Dimensions</i>	High-Level	Low-Level
	<i>Strategic</i> High-level information on changing risk The board	<i>Tactical</i> Attacker methodologies, tools and tactics Architects and sysadmins
Long-term Use		
Short-term Use	<i>Operational</i> Details of a specific incoming attack Defenders	<i>Technical</i> Indicators of specific malware SOC staff/ IR

the review are reflected by the research questions which are presented in the following Subsection.

The systematic review research process was led by the Kitchenham et al. guidelines [33] and is structured as stated in Fig. 2. First, the existing publications will be identified; second, the identified results will be screened to discard non-relevant literature; finally, the remaining results will be used to collect research data corresponding to our research questions, and the quality of the examined studies was assessed. The steps of this methodology are introduced in more detail in the following Subsections 3.2 to 3.5. The following subsection 3.1 introduces the underlying research questions.

3.1 Research Questions

Five research questions (RQ) were developed to represent the skeleton of fundamental research on CTI for hospitals. An additional question will guide the research to compare the findings with generic research findings on CTI. The questions are introduced in the remaining part of this subsection.

3.1.1 What Cyber Threat Intelligence (CTI) issues are addressed in the research, and in what clinical contexts do they arise? (RQ1)

First, the general focus of the research was determined. This includes the general focus of CTI research and clinical context. The CTI focus aims to determine the CTI phase (collection, processing, or dissemination). Findings on the clinical context will provide insight into whether the heterogeneity and uniqueness of hospitals are properly considered in the current research. This includes classifying the different sizes of hospitals, specific divisions and departments in hospitals, and the technical focus (IT or Medical Cyber Physical Systems (MCPS)/Operational Technology (OT)).

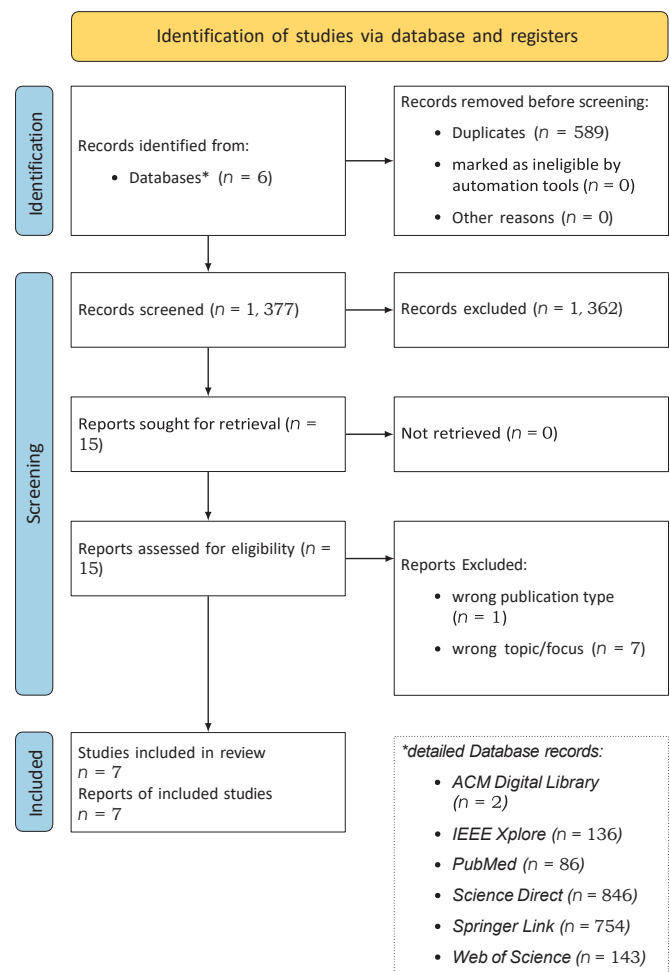


Fig. 2 PRISMA diagram displaying the process guiding the literature selection including the identification of literature, meta and full text screening.

3.1.2 Which types of medical or hospital-related devices are involved, and what role do they play in the studies? (RQ2)

The unique use of MCPS in hospitals was considered in the second RQ. The available and used MCPS are

heterogeneous. Hospitals use various products. Beginning on a more abstract level, the goal was to evaluate whether the identified research included medical devices and which devices were considered important or were the only devices with available data in the current research. The RQ does not aim at specific devices but rather at device classes. To answer this question, the devices were systemized into the following categories: patient criticality (non-patient critical, patient critical), physical application level (wearable, mobile, and stationary devices), and network status (not network-enabled, network-enabled).

3.1.3 What methodological approaches and types of studies are used to investigate CTI in the hospital setting? (RQ3)

In addition to topic-related focuses and contents, the scientific methodology used were evaluated (e. g, survey, proof of concept, literature review, use cases, case study, demo). The evaluation does not go into more detail about the quality of the methodologies used. We consider quality assurance to be a given due to peer reviews (see subsections 3.3 and 3.5 for additional statements related to this decision).

3.1.4 How is CTI defined in the studies, and are any specific standards or frameworks referenced? (RQ4)

Based on the findings of different studies that different understandings of CTI are in use, the underlying definitions of CTI were compared. In the same manner, the referenced or used CTI standards (e. g, STIX) were evaluated.

3.1.5 What data sources and real-world implementations of CTI are referenced, and which countries or healthcare systems do the studies focus on? (RQ5)

Finally, the connection between existing research and real systems was reviewed. The goal was to distinguish research based on the countries or healthcare systems that were the basis of the research. This may allow for the detection of existing regional differences and the identification and explanation of regionally limited research gaps. Second, to assess the implications for the real world, it is necessary to determine whether real world implementations or issues in implementing CTI were a basis for the existing research. This can help identify how practically driven research currently is.

3.1.6 How do the findings of CTI for hospital environments compare to general findings on CTI? (RQ6)

To amplify the research, existing findings of CTI in general should be interwoven with the findings and questions from the healthcare sector. For that, the general findings were compared and discussed based on the findings for the healthcare sector and existing preconditions.

3.2 Identification of Research

To gather relevant publications and ensure high recall, a combination of CTI terms and abbreviations, as well as hospital-related terms, was used as search strings. Each search string was a combination of hospital-related terms and "Threat Intelligence", "Cyber Threat Intelligence", and the abbreviation "CTI". The selection of hospital-related terms consisted of two groups of terms. The first group includes general terms that identify hospitals as a unit. The second group represents medical devices and is based on the findings of Weber et al. on synonymous terms [16]. The range of terms increased the probability of finding research on the topic that uses only less common terminology. Simultaneously, it increased the probability of false positives. As stated above, a high recall was deemed essential with respect to the expected low amount of research in this area.

The systematology for the search strings, including all terms, is stated in Table 2. These search strings were used as inputs in the following scientific search engines: IEEE Xplore, ACM Digital Library (The ACM Full-Text Collection), Science Direct, PubMed, Springer Link, and Web of Science. The libraries include databases with different focuses. This includes a technical focus such as in IEEE, ACM or a medical focus such as in PubMed. All databases accumulate to over 176 million entries. Whereby, the entries of all databases are presumably not disjoint. See Table 3 for individual sizes. Where possible, sensible and necessary, the search results were filtered according to the selection criteria, as stated in Table 3. This mainly includes limiting the results to articles that are written in English, published between 2020 and May 2025, and have a focus on computer science. When a database returned a small number of results, the field of research was not specified because manually excluding results from other fields was deemed practical and vice versa the "computer science" filter was just applied if the number of returned results was too big to handle manually without the filter. The queries were conducted at 18th, and 23rd June 2025 and resulted in 1,966 exported articles across all

Table 2 Searched strings used for querying research publications. Each String is a combination of a hospital related sub-string and a logical AND followed by "CTI", "Cyber Threat Intelligence", and "Threat Intelligence" separated by a logical OR. E.g, The full search string for S3 is: ("Health" OR "Healthcare" OR "Hospital") AND ("CTI" OR "Cyber Threat Intelligence" OR "Threat Intelligence")

#	Hospital related Sub-string	Results
S1	"Medical Cyber Physical Systems" OR "MCPS" OR "Medical CPS"	22
S2	"Internet of Medical Things" OR "IoMT"	85
S3	"Health" OR "Healthcare" OR "Hospital"	1,447
S4	"Connected Health" OR "Connected Healthcare" OR "Digital Healthcare"	40
S5	"E-Health Network"	2
S6	"Healthcare IoT-based Systems"	0
S7	"Healthcare 4.0"	12
S8	"Industrial Healthcare Systems" OR "Healthcare Systems"	169
S9	"Internet of Health Things" OR "Internet of Healthcare Things"	15
S10	"IoT Health"	6
S11	"Medical Sensor Networks"	4
S12	"Networked Healthcare"	3
S13	"Networked Medical Devices"	9
S14	"Smart Medical Devices" OR "Medical Devices"	152
Total		1,966

databases and query strings used. Most articles were obtained from searches using S3. This is reasonable because these are more general terms. All articles were screened for potential duplicates. This process was orchestrated using a two-fold procedure. First, duplicate entries were automatically detected and deleted based on different criteria: exact DOI match or exact match of title, authors, journal, and year. All remaining articles were manually checked in batches for similar articles. The similarity was classified based on the metadata (title, journal, year of publication, authors, pages, DOI, and abstract). This led to 589 deleted articles that were marked as duplicates, leaving 1,377 unique results for manual screening by the authors.

3.3 Selection

To ensure that only fitting and high-quality research on the topic is selected, the inclusion and exclusion criteria defined in Table 4 and Table 5 are applied to filter the initial results. This includes limiting the results to

Table 3 Databases, applied filtering criteria in each database, and databases sizes used for searches

Database	Filtering Criteria	Database Size (176,2 M)
ACM Digital Library	01/2020 - 05/2025	≈ 3.2 million publication records
IEEE Xplore	1 January 2020 - 31 May 2025	≈ 7 million documents
PubMed	1 January 2020 - 31 May 2025, english	≈ 39 million citations
Science Direct	2020 - 2025, english, computer science	≈ 18 million full-text articles
Springer Link	2020 - 2025, computer science	≈ 12 million documents
Web of Science	1 January 2020 - 31 May 2025	≈ 97 million records

a reasonable period of the last five years and to articles published only in peer-reviewed journals or conferences. Because the initial research suggested that the field does not offer many publications, the criteria were limited to CTI for hospitals. The integration of CTI has been proposed in the presented research [10–13]. Those publications included only one hospital specific CTI research citation by Javaid et al. who cite a paper by Sills et al. from 2020 [34]. This was obtained by snowballing. In the same manner, Sills et al. have not cited research that specifically discusses CTI for hospitals. Based on just one specific citation from 2020 from all three examined publications published in 2023 and 2024, there is no indication of relevant research beyond the scope beginning in 2020. Additionally, in a fast evolving field as computer science, older results may be less relevant. Therefore, the search was limited to publications from 2020 to May 2025, as the searches were conducted in June 2025. No further criteria were used to add further specifications.

The criteria lead to a content scope that limits research to publications specifically on CTI for hospitals without further restrictions. Research that mentions CTI but does not contribute in terms of content or handles CTI from a perspective other than computer science was excluded, as this research does not contribute to the introduced RQs. However, a soft and different use of the term CTI has not caused a decision to exclude research through the screening process. The criteria were applied in a two-step screening process in accordance with the guidelines of Kitchenham et al.

Table 4 Inclusion criteria applied to find relevant results

#	Criteria
I1	Research is published within January 2020 and May 2025
I2	Study is published and available in full length
I3	Study includes the searched terms (see Table 2) in title or abstract
I4	Study has focus in the field of computer science

Table 5 Exclusion criteria applied to keep only relevant results

#	Criteria
E1	Study is published other than in a peer-reviewed journal or conference
E2	Study is written in another language than english
E3	Study is a duplicate result
E4	Study has focus outside of the hospital context

In the first quantitative screening, the articles were screened by the three leading authors based on the title, abstract, and metadata (e.g. publication date, type of publication). Most articles were excluded in this step. After excluding 1,362 publications, 15 publications remained for the second screening stage. The first screening stage led to the identification of 18 alternative terminologies associated with the abbreviation CTI originating in different sciences (mainly computer and medical science, e.g. chest tube insertion, cardiac output time index, critical transportation infrastructure, cross technology interference).

The second stage involved searching for available full-text versions of the remaining papers. Full-text versions of all 15 publications were retrieved. The three authors screened the full text of each article, again checking for alignment with the criteria. Similarly to the first screening stage, all three authors screened each publication. This ensured that each decision was clear. However, each non-unanimously made decision was discussed to reach a consensus. Six articles that connoted differing fields with CTI or just mentioned CTI were excluded. This includes a result that connoted Threat Intelligence in the sense of AI methodology for cybersecurity in hospitals, rather than with the meaning underlying this research, or another publication related to quantum mechanics. In addition, another result was excluded. The result related to a conference was excluded as it represents a keynote and not a journal or conference paper. No other results from different fields were excluded. This led to the seven remaining articles for data extraction, which are presented in subsection 3.4.

Kitchenham et al. suggested Cohens Kappa [35] to reflect the decisions. However, Cohens Kappa is limited to two raters. Therefore, Cohens Kappa was replaced with Fleiss Kappa [36]. Thus, the decisions of all three raters were evaluated with a score of 0.81. This score can be related to an "almost perfect" strength of agreement based on the proposed benchmarks for Kappa statistics from Landis and Koch [37]. Absolute figures support this. Of the 1,377 anticipated decisions, only five were not unanimously approved. This was divided into four articles that were excluded and one included article.

To check for additional search terms, snowballing was applied to all remaining publications but this could not reveal additional paths to find other relevant literature. The remaining publications were traced back to evaluate their origins in a meta-analysis considering the databases from which the articles were sourced (see Fig. 3) and the search terms used in all databases (see Fig. 4). This showed that ACM and Science Direct had no impact on the results, nor did they have articles that met the criteria. IEEE Xplore inherited three articles, and Web of Science inherited four articles that match the criteria. The two databases in combination were sufficient for a search based on the defined criteria. Both inherited articles that build two disjoint sets. When shifting the view to the origin of the articles based on the search queries (SQ) used to find the articles in the databases, the query that incorporates the most general term-set, search query 3, is the leading query. All seven articles inherited one of the terms "health", "healthcare", or "hospital". Including this term set, only six of the 14 term sets provided results that matched the inclusion and exclusion criteria. "Smart medical devices" and "medical devices" provided half of the remaining results, respectively. Set 13, "Networked Medical Devices", set 9, "Internet of Health Things" and "Internet of Healthcare Things", set 8 "Industrial Healthcare Systems" and "Healthcare Systems", as well as set 2 "Internet of Medical Things", and "IoMT" each provided one article that matched the criteria.

3.4 Extraction & Synthesis:

The selected studies were systematically examined. This allowed a structured and objective analysis to gain necessary intel on the subject. This is achieved using objective criteria and information that support the research questions 3.1.1 to 3.1.5.

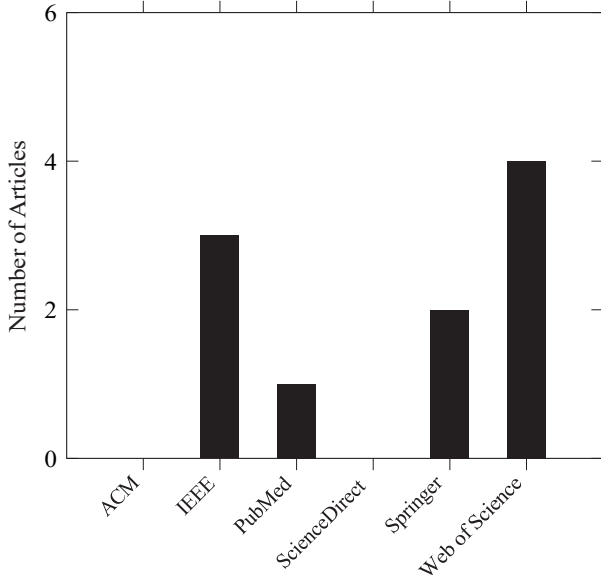


Fig. 3 Database-Origin of included articles, remaining after selection process.

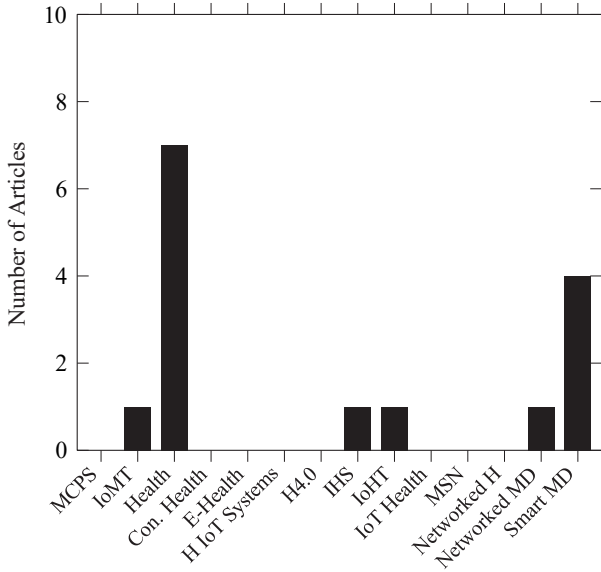


Fig. 4 Origin based on the search queries of included articles, remaining after selection process. Each entry represents a query which is build with the search terms correlated to the abbreviated term on the x-axis. The entries represent the queries in the same ordering as in Table 2. Introduction of new abbreviations: "H" represents healthcare, "MD" represents Medical Devices, "IHS" represents Industrial Healthcare Systems and "MSN" represents Medical Sensor Networks.

3.5 Quality Assessment

As proposed by Kitchenham et al. [33] a quality assessment should be conducted and can serve different purposes. The second most common purpose according to Zhou et al. [38] is to provide more detailed inclusion and exclusion criteria. This purpose was pursued by the exclusion criterion presented in E1 and by E4 and I4. E4 and I4 check for content-related alignment of the publications. E1 ensures that the studies have been checked by a peer-review process.

4 Results

The following subsections present the results over all examined publications for each research question.

4.1 Addressed research gaps – RQ1

The focus of research on CTI for hospitals is limited, similar to the number of results. Except for one article, all publications focused on the collection of CTI (as depicted in Table 6). Collection-focused publications include Al-Hawawreh et al [39], who presented the generation of actionable CTI. They described the collection of indicators for Intrusion Detection based on anomalies caused by different Ransom Denial of Service (RDoS) attacks on the Constrained Application Protocol (CoAP). However, they do not classify their results in terms of their integration in a larger scope of CTI (e.g., transforming the data into STIX). With that in mind, the authors emphasize giving a clear overview of CTI and drawing an outlook over the following steps, such as data transformation into CTI Standards or CTI sharing. By clearly classifying the contribution in the field of CTI, it is delimited between intrusion detection, or any other concept not necessarily connected to CTI, and CTI itself.

In addition to focusing on the collection of CTI, three publications also focused on processing and dissemination. Hatzivasilis et al. [40] mainly focused on collection, but also provided research on the processing of the collected data and the dissemination to form their swarm intelligence solution. The Blockchain-based environment proposed by Petru-Rosu et al. [41] collects data, but mainly focuses on secure sharing. Third, the SECANT platform [42] presents not only a collaborative collection of CTI. It also provides analysis and sharing functionality, thereby benefiting all three CTI phases.

Two articles presented additional processing steps after data collection. Sills et al. [34] augment the col-

lected data with results from Wikidata and public medical databases. Moreover, the connection between hacker threats and MITRE-ATT&CK was presented by Ampel et al. [43]. In addition, the methodology presented by He et al. is focused on processing [44]. The methodology integrates CTI into an Incident Response strategy to make it proactive. This is the sole publication without any work regarding the collection of CTI.

Three of the studies provided information on the technical focus (cf. Table 6). All three articles focused on OT, specifically medical devices [39, 41, 34]. This includes Al-Hawawreh et al. [39]. However, they did not present real medical devices in their setup. The remaining four publications did not specify whether the focus was on IT, OT, or both.

None of the publications introduced a limitation or specification for a hospital department or hospital size. In general, the heterogeneity of hospitals, considering their size and different departments, is not discussed in any of the publications.

4.2 Device Focuses – RQ2

Three articles discussed CTI content-wise and focused on OT (cf. subsection 4.1). Nevertheless, none of the publications specified specific medical devices. Instead, Al-Hawawreh et al. [39] specified that network-enabled devices are considered. Concrete devices were not introduced. In the same manner, Petru-Ruso et al. [41] also mentioned medical devices, but in addition to the limitation of portable and wearable devices, they did not make any other specifications. Sills et al. [34] simply mention medical devices without any specifications. All other articles [42–44, 40] provide no information on medical devices as part of the research.

4.3 Research Methods – RQ3

The methodologies of the articles are mainly practically aligned. All seven publications presented a proof of concept or concept, partly supplemented with a case study by Ampel et al. and He et al. [43, 44] or a demonstration by Petru-Ruso et al. [41]. The methodologies of the publications are presented in Table 6.

4.4 Definitions and Standards – RQ4

Although most articles presented a practical approach, only four publications refer to a data standard related to CTI. The used or just mentioned (CTI-related) data standards are listed in Table 6. STIX is mentioned by

all four publications [42, 34, 44, 40]. This includes Sills et al. [34], who refer to STIX by introducing Unified Cybersecurity Ontology 2.0 (UCO), which is based on STIX 2.0. Additionally, He et al. referenced Malware Attribute Enumeration and Characterization (MAEC), Cyber Observable eXpression (CYBOX), which is deprecated and now integrated into STIX, and TAXII for CTI exchange, which was also introduced by Hatzivasilis et al. [40].

In addition, Hatzivasilis et al. [40] integrated the Malware Information Sharing Platform (MISP), an open-source Threat Intelligence platform, into their Proof of Concept (PoC), as did Caballero et al. [42] and He et al. [44] in their concept. Additionally, MITRE-ATT&CK [39, 43], NIST Incident Response framework (framework of the National Institute of Standards and Technology in the United States of America) [44] and Cybersecurity Knowledge Graph [34] are integrated frameworks or concepts that are not specifically designed for CTI. Besides MISP and the other non-specific solutions, the remaining publications did not provide information about used technologies or data standards that are relatable to CTI.

The diverse use of the term Cyber Threat Intelligence or just Threat Intelligence is also represented by the investigated publications. Four articles did not introduce any of these terms or provided a definition [42, 41, 34, 40]. The remaining three articles provided definitions. The referenced definitions are stated in Table 6. However, He et al. [44] did not provide a source for their main definition. Nevertheless, they introduced different types of CTI and provided an article by Tounsi and Rais [45] as a reference. The same reference was introduced by Al-Hawawreh et al. [39]. In contrast, they used the main definition provided by Tounsi and Rais and did not introduce the different types of CTI. Supplementary, they also provided two other definitions: A definition published by the SANS (SysAdmin, Audit, Network, Security) Institute [46] and a definition presented by Yeboah-Ofori & Islam [47].

Finally, Ampel et al. [43] introduced a main definition provided by Ramsdale et al. [48]. In addition, they specify their definition and categorize different types of CTI based on Tounsi and Rais. All three articles utilize some part of Tounsi and Rais' definition. Nevertheless, all three articles referenced different sources for their main definitions of CTI.

4.5 Data Sources and Regional Focus – RQ5

Considering the sources of Threat Intelligence used in the publications, all provided information about their used data. The origin of the data used is presented in

Table 6 Source origins of integrated data, addressed regions, CTI phases, study types and content by each publication. Underlined entries mark the integration of sources which provide CTI by declaration. CTI phases include collection (C), processing (P), and dissemination (D).

Publication (year)	External data sources Own/Local data	Technical Focus CTI Phase	Data Standards used or just men- tioned	Associated Region/ Country	Study Type	Referenced Definitions	Content
Al-Hawawreh et al. [39] (2024)	✓	× C OT	N/A	N/A	Proof of Con- cept	Tounsi & Rais [45], SANS Whitepaper [46], Yeboah-Ofori & Islam [47]	modeling of attacks against CoAP and analysis of those attacks
Petru-Rosu et al. [41] (2024)	✓	× C OT P D	N/A	N/A	Proof of Con- cept/ Demo	N/A	blockchain based environment for secure shar- ing of medical device data
Sills et al. [34] (2020)	×	✓ C OT P	UCO 2.0	N/A	Proof of Con- cept	N/A	CTI repository including medical devices, their known vulnerabilities, integrated in a Cyberse- curity Knowledge Graph
Ampel et al. [43] (2024)	×	✓ C N/A P	N/A	case study related to US hospitals	Proof of Con- cept, Case Study	Ramsdale et al. [48], Tounsi & Rais [45] for introduction of CTI-Types	novel transformer and multi-teacher knowledge distillation design, to link hacker threats to MITRE-ATT&CK
He et al. [44] (2022)	×	✓ P N/A	MAEC, STIX, TAXII, CYBOX	case study in UK	Concept, Case Study	Tounsi & Rais [45] only for introduction of CTI-Types	proactive IR procedure based on NIST IR methodology, that integrates CTI
Hatzivasilis et al. [40] (2024)	✓	✓ C N/A P D	STIX, TAXII	proposal applied in Europe (EU)	Proof of Con- cept	N/A	swarm-intelligence solution that integrates CTI, including automation for risk assessment, event evaluation processes, and IR
Caballero et al. [42] (2022)	✓	✓ C N/A P D	STIX	underlying project with focus on Europe (EU)	Proof of Con- cept, Imple- mentation	N/A	platform for collaborative CTI collection, anal- ysis and sharing,
Sum	4	5	C6- P6 D3	-	-	3	-

Table 6 and is declared in more detail in the following paragraph.

The articles presented a diverse combination of data sources. Four of them generated data or proposed to collect data based on local devices in healthcare [39, 42, 40, 41]. Whereby Petru-Rosu et al. [41] presented a collector as part of a concept, but did not provide further information on data collection. Likewise, Hatzivasilis et al. did not specify further their local data collection. On the other hand, Al-Hawawreh et al. generated CTI by simulating attacks [39] and Caballero et al. [42] used CTI generated from device and software-logs, as well as alerts and a manual collection.

External sources were also common. This includes

- the collection by crawling security websites, forums and social media from surface and dark web [42],
- the collection of manufacturer data (Phillips, GE, Medtronic), data from CISA ICS-CERT and more not specified sources augmented with data from Wikidata and public medical databases [34],
- from hacker forums enriched by CVEs and related MITRE-ATT&CK tactics [43],
- from MISP, US/UK-CERT, security incident reports and MITRE [44]
- and from Healthcare Information Sharing and Analysis Centers (ISACs), CVEs, sectorial repositories and the dark web [40].

The CTI used, generated, and/or applied was mostly not equipped with a restriction or focus on a specific country or region. Only Caballero et al. [42] presented a project focus on Europe, but did not restrict the research presented with any regional restrictions. Additionally, He et al. [44] presented their case study located in the UK and Ampel et al. [43] presented a case study linked to vulnerabilities in hospitals in the United States of America. Hatzivasilis et al. [40] presented that the proposal is applied in a supply-chain of european healthcare organizations und consideration of EU data protection regulations.

None of the publications presented real world applications of the proposed frameworks. However, some presented resulting implementations that could be applied in real world scenarios. This includes a Threat Intelligence Module (TIM) to gather, to provide a dashboard, and display CTI presented by Caballero et al. [42]. Petru-Rosu et al. presented a Blockchain for data transfer and epsilon privacy [41] and Sills et al. demonstrated a system to crawl data from different sources, which can enrich the results with data from Wikidata for devices gathered from the Global Unique Device Identification Database (GUDID). [34]. Lastly, Ampel et al. presented an artifact connecting hacker threats

ATT&CK-Link [43] and Hatzivasilis et al. illustrated their AI4HEALTHSEC swarm intelligence framework where CTI is incorporated in risk assessment and event evaluation processes [40].

4.6 Sector uniqueness – RQ6

When comparing the findings for hospitals with those of the results in general, similarities are visible. The missing representation of the organizational perspective was also present in research for healthcare. Research based on a methodology that incorporates a survey among hospitals or healthcare specific cyber (security) services could not be identified. Additionally, the diverse understanding of "Cyber Threat Intelligence" is not just a problem in general research. Missing introductions of definitions of key terminology and in case of presented definitions, diversely sourced and heterogeneous definitions suggest that the missing common ground in defining CTI seems to be unsolved in research specifically for hospitals too. When shifting the view to more technical aspects, in contrary to general research, twitter seems absent as a source for the collection or generation of CTI. In the same manner, Threat Reports were not as dominant, but (hacker) forums were of interest. A technical uniqueness, medical devices, was not present with a classifying discussion that distinguishes medical devices from other OT. Medical devices were mentioned, but were not subject to a detailed comparison or consideration. This also correlates with the general findings that the perspective of organizations was often missing. The specific perspective of hospitals was missing in hospital specific research too.

5 Discussion

Hospitals are an obligatory unit that provides vital services to a society and a human being, therefore, they are available in almost every country [49], and research suggests the implementation of CTI. Despite that, research on CTI is limited. The small amount of research could be due to the lack of CTI demand for hospitals. As mentioned above, the demand for CTI itself has been proposed several times, and a broad implementation of CTI has not been detected in the literature. This indicates that the research gap in CTI for hospitals persists. At the same time, due to the limited amount of research, it follows that the conclusions that can be drawn are limited. This has effects on the variety of conclusions that can be drawn and on the resilience of each conclusion. Additionally, the missing reports of

real life implementations may imply that generic solutions are not suitable, as well as the findings of Irfan et al. [29] on the need of solutions tailored to organizations. Finally, the rare research results currently are mainly published in journals and conferences with a focus on computer science. Currently there is no indication that researchers are focusing specifically healthcare informatics, or medical focussed destinations for publications. This could indicate that the corresponding research groups are mainly based on computer scientists.

5.1 Grasp of CTI

Furthermore, a different interpretation of CTI and the use of key terms related to CTI in general could structurally slow down research and make research inefficient. Definitions of CTI and key terms are not provided consistently in the examined research or different explanations for the terms are presented. For example, Ampel et al. [43] presented operational CTI as *"[it] relates to the impending attacks against an organization"*, which is in contrast to the description of the subtype given by Chismon and Ruks (see Subsection 2). Additionally, different thematically oriented research areas connote "Threat Intelligence" with different meanings, like an excluded paper by Trivedi et al. [50] which is related to Artificial Intelligence methodology for cybersecurity in hospitals. Therefore, the following part is dedicated to providing a definition of CTI including key terminology. The key principles are:

1. respecting the origin of intelligence to maintain coherent definitions in related fields,
2. avoiding ambiguous terminology to enable straightforward communication within and beyond the research community, and
3. keeping it simple to prevent misunderstandings and provide easy access for non-specialists.

Following this scheme, the findings presented in Section 2 are incorporated into the following definition. It is based on the definition proposed by Sakellariou et al. [26] and Saeed et al. [20]. The proposed definition changes two key points: It introduces each term that is related to the concept inside the definition (e.g. Sakellariou et al. make use of "CTI sources" which is a term that they only separately define) and it incorporates additional descriptive terms given by the US Army [30]. Additionally, this leads to the integration of the following three principles: The following definition sets the basic principle to the process perspective as in the definition of Saeed et al. because this perspective can be seen as a superset for the remaining perspectives. Secondly, the definition clearly states the goal as

proposed by Sakellariou et al. to ensure a sharp understanding of the purpose of the process. Third, the definition integrates the sub-process of transforming data into intelligence into the definition to comprehensively distinguish the terms. Following this, we propose the following definition:

"Cyber Threat Intelligence (CTI): is a process pursued by a CTI-Team to integrate, evaluate, and distribute intelligence to identify, monitor, and anticipate cyberthreats, threat actors and their motivation, methodology of cyberattack, and victims to support defenders towards detecting, preventing, or (ideally) predicting a cyber-attack and making appropriate decisions. Intelligence is transformed out of information or data by collecting, processing, assessing, and analyzing it. A CTI-Team can create intelligence or consume already available intelligence.

Additionally to a CTI-Team, CTI encompasses three main perspectives (based on Lowenthal [31]):

- a process (Cyber Threat Intelligence or threat intelligence process [26])
- a product (Intelligence or CTI product [26])
- an organization/team (Cyber Threat Intelligence - Team (CTI-Team))"

Furthermore, more terms can be defined to describe different aspects of the process like presented by Sakellariou et al. [26], like CTI source, CTI product or CTI producer, CTI consumer or CTI system. The process is realized by a Cyber Threat Intelligence Platform (CTI-Platform) which can provide functionality for collection, information/presentation, or dissemination/sharing. The module inherently connected to serve the purpose is the information platform.

Gaining intelligence is not self-served by collecting data. Intelligence is subject to quality criteria: accuracy, timeliness, usability, completeness, precision, and reliability. Effective intelligence is relevant, predictive, and tailored (condensed from the US Army by Ainslie et al. [21]). This distinguishes data and intelligence. "Data and information are not intelligence." [21]. This quote from Ainslie et al. can be described more precisely: Data and information are not necessarily intelligence. However, intelligence may contain data and information. Intelligence can serve different purposes, or groups that deal with intelligence and by which occur in different molds of representation. Therefore, intelligence is categorized into strategic, tactical, operational, and technical intelligence. The subtypes are classified by their time of use and their level of abstraction, as stated in table 1.

The CTI-Team performs the different parts of the process. Even though sub-processes can be automated (e.g. collection of data or sharing of intelligence). Ideally, the team can aggregate intelligence by an intelligence exchange within a sharing network and intelligence gained based on their own data (e.g. by analyzing network traffic).

The terminology introduced beforehand should sufficiently support sharpening the basic understanding of CTI. However, the basic nature of the terminology introduced delimits its applicability. More detailed concepts and definitions (e.g. the complexity factors and the reference model by Sakellariou et al. [26]) are necessary for specialized research. Additionally, the key terminology should not only be a basis for efficient collaborative research efforts in this field. It should be introduced in the corresponding publications to classify the presented research and the limitations inside the field. For example, the generation of indicators by Al-Hawawreh et al. [39] is placed within the field of CTI research. Clearly defining CTI, and terminology as well as classifying the research within the field as a collection methodology could clear the limitations.

To classify all articles examined, we have assigned the articles to the CTI perspectives they approach. The assignments and short descriptions are presented in Table 7. For example, the generation of indicators mentioned above by Al-Hawawreh et al. can be classified as the perspective of Intelligence. Although this classification is straightforward, other decisions are not as clear. Sills et al. presented a process that collects and enriches information or intelligence to generate intelligence of higher quality. The process is conceptualized to be automated. Therefore, it also logically serves the process. Similarly, with respect to the argument that each approach aims at improving CTI, it is also possible to argue that all publications serve the CTI-Team. We note that there is room for different arguments that lead to different classifications. The main goal of classifying the research in that way is not to gain absolute interpretations, but rather to generate an improved presentation of approaches. This can lead to better comprehension by the readers and better awareness of the corresponding authors. Overall, this could prevent misconception caused by ambiguous usage of the CTI terminology just as in a publication by Trivedi et al. [50]. They have reviewed research on AI techniques for cybersecurity for Remote Patient Monitoring Systems (RPMs) presented as "AI-enhanced Threat Intelligence". In addition to the option presented above to classify research, more technical classifications can be introduced such as, for example, the phases of CTI as presented in 4.1. Those classifications reveal that only a minority of the

reviewed publications have focused on the sharing of CTI as only 3 focused on dissemination. Additionally, 6 publications processed intelligence in some way with a focus on the process. Still, processing under the perspective of a CTI-Team could be regarded more as an action that prepares intelligence for human consumption. In conclusion, CTI research demands a classification or interpretation under different perspectives that are not final but support a better understanding of the field and of a broader picture.

5.2 CTI Sharing

In the same manner, sharing standards should be introduced where possible and necessary. In practice, effective CTI is only possible when a collective effort is the basis of the work. A data breach, anomaly, or finding from one organization (e.g. a hospital, vendor, or service provider) could provide predictive information to protect another entity within the sharing network and vice versa.

Following this scheme, consistently building sharing networks does not only include hospitals. The aspect of the supply chain and adjacent entities is vital for cybersecurity of hospitals. This encompasses not only building networks that include the entities, but also presenting research that considers those aspects and, therefore, widens the view. The entities to be considered are (not exhaustive list): Manufacturer of medical devices, manufacturer of IT infrastructure, medical or IT service providers, emergency services, medical offices, and health insurance companies. All of them provide either products that are technical entities in a hospital network infrastructure or feed data into the network. An example for incoming data is patient data collected in a preclinical treatment by emergency services, provided to the hospital [51]. Having these benefits considered, considering the risk of disclosing information by sharing self-gained intelligence should always be part of research and practice.

5.3 User-Centered Intelligence

Based on the focus on protecting critical data, research should focus on automated generation of intelligence based on medical devices and network traffic produced by those devices. The automated generation should consider GDPR and NIS2 conform transformations of data into intelligence. In general, this could support current research that is influenced by practical approaches such as collecting intelligence. However, user centered approaches that put hospitals at the center of investiga-

Table 7 Mapping of examined research and CTI perspectives: Cyber Threat Intelligence (Process), Intelligence (Product) and CTI-Team; rated as: ● approaches from perspective, ½ partially approaches perspective, ○ does not approach perspective

Publication (year)	Perspective			Classification/ Delimitation
	Process	Product	Team	
Al-Hawawreh et al. [39] (2024)	○	●	○	gained intelligence in form of IoC by simulating attacks; did not classify their results regarding the context of CTI
Petru-Rosu et al. [41] (2024)	●	○	○	blockchain based environment supports sharing process, the process handles Intelligence but research does not focus on collection or production of Intelligence
Sills et al. [34] (2020)	½	●	○	aggregation of information and intelligence, as well as enriching those serves promoting the product, automated solution also serves the process
Ampel et al. [43] (2024)	½	●	○	knowledge distillation and linking to hacker threats serves the product, automated solution also serves the process
He et al. [44] (2022)	●	○	○	integration of CTI into IR procedure serves the process
Hatzivasilis et al. [40] (2024)	●	○	○	focus on sharing, IR procedures and risk assessment presents a dedication to the process
Caballero et al. [42] (2022)	●	●	○	platform for collection, analysis and sharing serves the process, at the same time collection serves the product

tions are not recognizable in the current research. Hospitals and their real infrastructure are not presented as a basis for research in the field of CTI. This means that current solutions are only loosely coupled to real world scenarios. However, solutions prove their value only when they fit in real world scenarios. The infrastructure with the devices in use and the correlated requirements, approaches, and standards is vital to inventing practical solutions that will essentially enter the praxis as hospital infrastructures are minted by OT (MCPS). Those MCPS are special compared to other OT. MCPS are embossed by different Standards (e. g. IEC 62304, ISO 14971, IEC 80001) and protecting them is uniquely critical. Measures have to be implemented with special caution as each measure could jeopardize patients.

Besides adapting and sharpening the current research focuses, creating solutions that allow the processing of intelligence should also play a vital role in the future. Current solutions have not focused on the creation of solutions on information modules. But with a rising amount of data and consequently following more intelligence data, suitable perspectives to filter, sort, and prioritize intelligence and overall display the intelligence in a user-centered design will become more important and eventually essential for functioning solutions.

6 Conclusions

Despite the inherent relevance of uninterrupted hospital operations and the determined cyberthreats hospitals face, CTI for hospitals is not sufficiently represented in research. Although CTI was recommended several times as a measure against cyberthreats for hospitals, the results in recent research are limited. The structured literature review identified only seven publications examining CTI specifically for hospitals from 2020 to May 2025. All conclusions drawn are subject to the limitation that is given by this limited amount of research. The published research articles range from holistic platforms or sharing (network) approaches to the generation of intelligence based on specific attacks or from specific sources. This includes mining intelligence data from hacker threats [43], RDoS attacks on CoAP [39], securely sharing intelligence data in a blockchain environment [41], aggregating medical devices and their known vulnerabilities [34], integrating intelligence in a proactive incident response process [44], a proposed method for swarm-intelligence, that integrates intelligence and AI/ML incorporated in a risk assessment and event evaluation process [40], or in a similar approach a solution for collaborative collection of intelligence, analysis, and sharing [42].

A missing sufficient consideration of key terminology connects all publications, as well as a missing perspective of hospitals. Only three articles presented their underlying definition, with all three referring to differ-

ent definitions. Likewise, only Ampel et al. [43] and He et al. [44] included case studies as a measure to correlate with real world scenarios. Generally speaking, overall the recent research misses the perspective of real world hospitals.

Based on these findings and the findings of CTI research outside of the hospital or health context, this article detected several issues related to current research and proposed strategies to improve current research with the goal of helping hospitals in the real world to implement CTI successfully. Those strategies cover consistently including and describing solid CTI terminology and prioritizing the organizational perspective, and thus the reality of hospitals. Through this, future research can align with real world issues of hospitals and their practitioners. Furthermore, the presented definition should be evaluated through experts or empirical testing to assess whether our propositions, which are based on our findings, show validity when applied. Moreover, the research community can collectively promote strategic and efficient research based on a common understanding of the field and key terminology.

Future research must consider real world devices, techniques and standards when collecting intelligence and selecting, using, or adapting sharing standards. This includes answering two key questions: First, do the current standards allow a sufficient integration of intelligence created inside the medical context? And second, are the current standards prone to disclosing critical data that is worthy of protection, and how can these data be protected by design by pseudonymization or anonymization?

Besides key issues related to intelligence collection, research should focus on solutions that allow adequate data handling in praxis. Analysts have to be able to handle large amounts of intelligence by prioritizing the incoming data. Filtering, sorting, and user-centric representation of information are key to intelligence handled by humans. Of course, collection and processing can be assisted by AI and, if suitable, can be automated to relieve human resources. This must align with the condition that the treatment of human beings within hospitals is always the main focus of hospitals.

The article determined the lack of CTI research specifically for hospitals and this research is also limited by that. It is also limited by comparisons and derivations from general CTI research. Future research could focus on comparing requirements in different sectors of critical infrastructure that are also minted by OT (such as the energy or water sector). This requires systematically evaluating the results from the other sectors.

To summarize, this article determined that the available research is limited and that the highly critical sec-

tor is insufficiently researched. The article proposes a short and adapted definition for CTI to create a basis for future research and classifies the examined research based on the presented definition. Additionally, even though research is limited and conclusions that can be drawn are limited, the article identified methodical trends and deficits in available research that lead to the following vital points for future research: First, hospitals and their needs must be a first priority in research. Second, medical devices as a source of intelligence have to be evaluated and checked for specific requirements. Third, clear and common definitions of CTI and related terminology are key to efficient research.

Acknowledgements We gratefully acknowledge Amelie Brucker and Tobias Müller from the MedSec research group for their proofreading and constructive feedback during the preparation of this paper.

References

1. Entwicklung der Lebenserwartung in Deutschland. <https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Sterbefaelle-Lebenserwartung/sterbetafel.html>
2. H.E. Kru"ger-Brand, Deutsches Ärzteblatt **111**(50), (2014)
3. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (2015)
4. Presidential policy directive/PPD 21—Critical infrastructure security and resilience (2013)
5. V. Sunil, S.P. Mathew, Acta Medica International **11**(1), 1 (2024). DOI 10.4103/amit.amit.7.24
6. I. Lella, DOI 10.2824/0710888
7. Cybersecurity in healthcare - European Commission. https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en
8. Microsoft Digital Defense Report. Tech. rep., Microsoft (2024)
9. S.T. Argaw, N.E. Bempong, B. Eshaya-Chauvin, A. Flahault, BMC Medical Informatics and Decision Making **19**(1), 10 (2019). DOI 10.1186/s12911-018-0724-5
10. A.A. Salami, U.T.I. Igwenagu, C.E. Mesode, O.O. Olaniyi, O.B. Oladoyinbo, Journal of Engineering Research and Reports **26**(5), 304 (2024). DOI 10.9734/JERR/2024/V26I51156
11. M. Aminu, A. Akinsanya, O. Oyedokun, O.T. Akinwande, Iconic Research And Engineering Journals **8**(2), 74 (2024)
12. S. Sarowa, B. Bhanot, V. Kumar, M. Kumar, in *Proceedings - IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT 2023* (Institute of Electrical and Electronics Engineers Inc., Dehradun, 2023), pp. 160–165. DOI 10.1109/DICCT56244.2023.10110141
13. M. Javaid, A. Haleem, R.P. Singh, R. Suman, Cyber Security and Applications **1**, 100016 (2023). DOI 10.1016/J.CSA.2023.100016
14. S. Weber, M. Pilgermann, S. Stein, T. Schrader, (2024). DOI 10.25933/opus4-3207

15. P. Koster, in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*, ed. by J. Soldatos, I. Praça, A. Jovanović (Now Publishers, Delft, 2021), pp. 978–1–68,083–823–7.ch17. DOI 10.1561/9781680838237.ch17
16. S.B. Weber, S. Stein, M. Pilgermann, T. Schrader, *IEEE Access* **11**, 41796 (2023). DOI 10.1109/ACCESS.2023.3270225
17. T.D. Wagner, K. Mahbub, E. Palomar, A.E. Abdallah, *Computers & Security* **87**, 101589 (2019). DOI 10.1016/j.cose.2019.101589
18. D. Balson, W. Dixon, *Cyber information sharing: Building collective security*. Report, World Economic Forum (2020)
19. S. Jimo, T. Abdullah, A. Jamal, in *Cybersecurity in the Age of Smart Societies*, ed. by H. Jahankhani (Springer International Publishing, Cham, 2023), pp. 451–467. DOI 10.1007/978-3-031-20160-8_26
20. S. Saeed, S.A. Suayyid, M.S. Al-Ghamdi, H. Al-Muhaisen, A.M. Almuhaideb, *Sensors* **23**(16), 7273 (2023). DOI 10.3390/s23167273
21. S. Ainslie, D. Thompson, S. Maynard, A. Ahmad, *Computers & Security* **132**, 103352 (2023). DOI 10.1016/j.cose.2023.103352
22. V. Jesus, B. Bains, V. Chang, *Ieee Transactions on Engineering Management* **71**, 6854 (2024). DOI 10.1109/TEM.2023.3279274
23. J. Rajamäki, D. Jarzemski, J. Kucera, V. Nyman, I. Pura, J. Virtanen, M. Herlevi, L. Karlsson, *WSEAS TRANSACTIONS ON COMPUTERS* **23**, 1 (2024). DOI 10.37394/23205.2024.23.1
24. R. Riesco, X. Larriva-Novo, V.A. Villagra, *Telecommunication Systems* **73**(2), 259 (2020). DOI 10.1007/s11235-019-00613-4
25. V. Mavroeidis, S. Bromander, in *2017 European Intelligence and Security Informatics Conference (EISIC)* (2017), pp. 91–98. DOI 10.1109/EISIC.2017.20
26. G. Sakellariou, P. Fouliras, I. Mavridis, P. Sarigianidis, *Electronics* **11**(9), 1401 (2022). DOI 10.3390/electronics11091401
27. P. Santos, R. Abreu, M.J.C.S. Reis, C. Serodio, F. Branco, *Sensors* **25**(14), 4272 (2025). DOI 10.3390/s25144272
28. M.R. Rahman, R. Mahdavi-Hezaveh, L. Williams, in *2020 International Conference on Data Mining Workshops (ICDMW)* (2020), pp. 516–525. DOI 10.1109/ICDMW51313.2020.00075
29. A.N. Irfan, S. Chuprat, M.N. Mahrin, A. Ariffin, in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)* (2022), pp. 1295–1300. DOI 10.1109/ICTC55196.2022.9952616
30. *INTELLIGENCE*, vol. 2–0 (United States Army, 2019)
31. M.M. Lowenthal, *Intelligence : From Secrets to Policy 7th Edition* (Los Angeles, California : CQ Press, an imprint of SAGE Publications, Inc., Los Angeles, 2017)
32. D. Chismon, M. Ruks, *MWR InfoSecurity Ltd* **3**(2), 36 (2015)
33. B. Kitchenham, S. Charters, *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Tech. rep., University of Durham (2007)
34. M. Sills, P. Ranade, S. Mittal, in *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)* (IEEE, Arlington, VA, USA, 2020), pp. 1–6. DOI 10.1109/ISI49825.2020.9280482
35. J. Cohen, *Educational and Psychological Measurement* **20**(1), 37 (1960). DOI 10.1177/001316446002000104
36. J.L. Fleiss, *Psychological Bulletin* **76**(5), 378 (1971). DOI 10.1037/h0031619
37. J.R. Landis, G.G. Koch, *biometrics* pp. 159–174 (1977)
38. Y. Zhou, H. Zhang, X. Huang, S. Yang, M.A. Babar, H. Tang, in *Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering* (Association for Computing Machinery, New York, NY, USA, 2015), EASE '15, pp. 1–14. DOI 10.1145/2745802.2745815
39. M. Al-Hawawreh, N. Moustafa, J. Slay, *Neural Computing and Applications* **36**(1), 15 (2024). DOI 10.1007/s00521-021-06441-5
40. G. Hatzivasilis, E. Lakka, M. Athanatos, S. Ioannidis, G. Kalogiannis, M. Chatzimpirros, G. Spanoudakis, S. Papastergiou, S. Karagiannis, A. Alexopoulos, D. Amelin, S. Kiefer, *International Journal of Information Security* **23**(4), 2951 (2024). DOI 10.1007/s10207-024-00869-1
41. A. Petru-Rosu, T. Tataru, J. Zelenjak, R. Kromes, Z. Erkin, in *2024 IEEE International Workshop on Information Forensics and Security (WIFS)* (IEEE, Rome, Italy, 2024), pp. 1–3. DOI 10.1109/WIFS61860.2024.10810716
42. M. Caballero, D. Kavallieros, A. Spyros, A. Tavernarakis, A. Tziouvaras, S. Bonacina, K. Chandramouli, M. Coroiu, L. Chen, T. Dounia, I. Giannoulakis, N. Gligoric, E. Kafetzakis, T. Kasig, V. Koumaras, T. Krousarlis, K. Lapidaki, A. Markakis, S. Marin, M. Manulis, S. Menesidou, S. Nifakos, L. Meng, S. Mhiri, M. Nati, K. Ntafloukas, D. Oniga, D. Papamartzivanos, S. Papastergiou, K. Sanchez, C. Sakkas, K. Stelliou, L. Trujillo, T. Tsikrika, E. Venegas, S. Vrochidis, D. Xydias, in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)* (IEEE, Rhodes, Greece, 2022), pp. 104–111. DOI 10.1109/CSR54599.2022.9850319
43. B.M. Ampel, S. Samtani, H. Zhu, H. Chen, J.F. Nuna-maker, *Journal of Management Information Systems* **41**(1), 236 (2024). DOI 10.1080/07421222.2023.2301178
44. Y. He, L. Maglaras, A. Aliyu, C. Luo, *Security and Communication Networks* **2022**, 1 (2022). DOI 10.1155/2022/2775249
45. W. Tounsi, H. Rais, *Computers & Security* **72**, 212 (2018). DOI 10.1016/j.cose.2017.09.001
46. R. Brown, R.M. Lee. *The evolution of cyber threat intelligence (CTI): 2019 sans CTI survey*. SANS Institute (2019) (2019)
47. A. Yeboah-Ofori, S. Islam, *Future Internet* **11**(3) (2019). DOI 10.3390/fi11030063
48. A. Ramsdale, S. Shiaeles, N. Kolokotronis, *Electronics* **9**(5), 824 (2020). DOI 10.3390/electronics9050824
49. Key table Hospital beds. <https://www.destatis.de/EN/Themes/Countries-Regions/International-Statistics/Data-Topic/Tables/BasicData/HospitalBeds.html>
50. J. Trivedi, M. Tahir, J. Isoaho, *IEEE Access* **13**, 106465 (2025). DOI 10.1109/ACCESS.2025.3572626
51. *Ergebnisse der Orientierungsstudie BSI-Projekt 453: eMergent-Digitalisierung im Rettungsdienst*. Tech. rep., Bonn (2023)