Mapping the cyber threat landscape in the healthcare using GDELT: A multimethod approach

Abstract: **When critical national infrastructure (CNI) such as hospitals is targeted by cyber-attacks, it poses a significant threat to the safety and well-being of individuals, as evidenced by incidents like WannaCry. To better understand vulnerabilities within the healthcare sector and develop preventative measures, it is crucial to examine the evolving nature of cyber threats and the types of attacks occurring. By adopting a multi-method approach comprising Social Networks Analysis, Natural Language Processing and Machine Learning, we use data from GDELT (Global Data on Events, Location, and Tone) to identify the prevalent attacks against hospitals while considering the type of attack and its date. Through this approach, we aim to unfold the meaningful patterns in cyber-attack evolution by analysing the relationships between emerging cyber-attacks mentioned in news reports. Our findings show that there is a significant increase in the number of attacks from 2017 to 2023. Also, hospitals are more prone to critical attacks such as cyber terrorism/state actor-sponsored criminal activities, APTs, DDoS. Mapping real-time data from diverse sources facilitate the initial determination of necessary cyber defences and inform the development of policy interventions to enhance the cybersecurity of Critical National Infrastructures.**

Keywords: **Cyber threat landscape, critical national infrastructure (CNI), GDELT, hospitals, social networks analysis, natural language processing, machine learning**

Introduction

The Critical National Infrastructure (CNI) comprise the pivotal systems in a country that enable the effective functioning of the society – these include systems that provide electricity, healthcare services, water, or telecommunication services [1]. Historically, there was a huge focus on physical assets and its protection that was concerning the CNI, however, this view has changed considering the digital transformation and the dependence on digital infrastructure. These systems are now evolving at a rapid pace, and hence, a holistic view of the threat landscape is required to manage and ensure the decrease of risks associated with the CNI [2]. A particular sector that is targeted by attackers is the healthcare sector. Since the WannaCry attack, there has been a huge increase in the number of cyber-attacks against hospitals. Indeed, the European Union's Cybersecurity Agency (ENISA) has suggested that nearly 53% of the cyberattacks in the EU are targeted at healthcare organisations [3].

Hospitals are complex organisations [4] with a unique mission and operating in a context where allocation of resources is crucial to the delivery of clinical care, clinical research and education. In this context, cybersecurity represents a challenge where hospitals do not have adequate resources to mitigate cybersecurity vulnerabilities such as budgets [5], technical know-how [6] and consequently, an understanding of the threats [6] thereby lagging

behind other industries [7]. The impact of cyber-attacks on hospitals is more profound and its ramifications can go beyond monetary or reputational damage. Studies have shown the negative impact of these attacks on patient outcomes as evidenced by the 2022 attack on the NHS UK's 111 service which was not operable thus inhibiting thousands to not receive the care during the pandemic [8]. For instance, delay in receiving medical care led to the death of patients due to ransomware attacks [9].

Countering cyber threats and preparing organisational and industry-wide strategies require up-to-date empirical data to better map the types of attacks that are prevalent for specific sectors [10]. Decisions pertaining to cybersecurity necessitates that accurate data is gathered from the triangulation of various sources, with tasks that aggregate abstract and complex information and enrich the information presented. Most of these decisions are based on conventional signals with organisational-level data on the threat signals received through the Intrusion Detection Systems (IDS) for comparing traffic patterns against the baseline data. This does not include unconventional signals through other media sources and news outlets that are not linked specifically to known vulnerabilities that are within the targeted organisation. While not all unconventional signals can be particularly useful or effective, and collating this is challenging and expensive, this is crucial for progressing the scientific understanding and mapping of the threat landscape. As such, several researchers argue that there is a lack of dependable data and lack of trust-worthy data sources specially to show the evolution of threats mapping both regional and industry-specific contexts [11, 12, 13].

Bridging this specific gap, our study develops and implements a multi-method framework to explore the trends of cyber-attacks on global hospitals from 2017 to 2023, with particular focus on identifying patterns and relationships between different types of attacks and hospitals. We utilise unconventional data sources obtained through GDELT database. GDELT is the Global Database of Events, Language and Tone and is an open platform where organisations, news, locations, themes, people, quotes or images that drive the society can be extracted and identified. GDELT had been used by several researchers to map and predict events such as social unrest [14], future violence levels in specific regions [15], stock market prices [16]. This study employs social network analysis (SNA), machine learning (ML) and natural language processing (NLP) methods to collect real-time data from several sources, obtain data on past cyber-attacks, classify these attacks based on their severity, and analyse the evolving threat landscape.

Our study contributes to the health cybersecurity research domain in two distinct yet interconnected ways. First, it provides a robust methodological framework that enables enhanced threat detection and response through real-time data collection and pattern identification. Second, practitioners and organisations benefit from this research as the framework allows for better risk assessments and data-driven decision-making, helping overcome uncertainties in predicting cyber-attack trends and becoming more proactive in reducing failure rates [17]. This enables healthcare organisations to identify potential vulnerabilities, anticipate threats, and implement proactive measures while effectively prioritising their resources. This systematic approach to understanding the threat landscape is fundamental for safeguarding the critical infrastructure and ensuring continuum of care for the patients.

The remainder of the paper is organised as follows. The next section discusses about the literature around cybersecurity in hospitals and summarises the recent attacks against hospitals. The third section will outline the data, and the methodology used to identify the cyber threat landscape followed by the results. The final section provides a discussion, limitation, and conclusion outlining the contribution to cybersecurity research and implications.

Cyber and hospitals

Cyber-attacks against hospitals have become an alarming global issue, with a growing number of incidents resulting in significant consequences for healthcare institutions, their patients, and staff [18]. This is concerning, especially, considering the emergence of new technologies such as robotics, Artificial Intelligence (AI), wearable devices etc. introduces new concerns about data privacy and security with the need to protect sensitive data [46].

The integration of new technologies with legacy infrastructure creates a complex ecosystem vulnerable to attacks [19,20,21]. These attacks can be classified based on their severity as outlined in the Cyber Incident Response Plan (CIRP) [22]. The CIRP outlines how organisations respond to cybersecurity incidents and is written to ensure that the incidents cause minimal damage to the organisation. Understanding the CIRP and creating clear processes, roles and responsibilities will enable organisations to understand the communication plans and the standard operating procedures (SOPs), understand the source of the incident and ensure that steps are taken to contain the threat and isolate the enterprise from the attacker. The CIRP classifies attacks based on the impact to the organisation and there are four levels of attacks outlined [22]. Level 4, *Critical attacks* are defined as those attacks where the impacts are catastrophic and can pose a threat to the life of individuals (patients in our case), cause significant destruction to the hospital capabilities and their IT applications/systems with a significantly huge reputational and financial loss [22]. Level 3, *High severity attacks* are defined as those where the impacts are "substantial to the proper conduct of" hospitals and can cause "impactful destruction" to the hospital capabilities and their IT applications or systems with a substantial reputational and financial loss. In our context, Critical and High severity attacks are primary infiltration attacks and include those where patients are directly impacted and can include for instance, disruption of critical medical equipment or even compromising patient records [22, 23]. The level of severity for critical or high depends on their impact. Level 2, *Moderate severity attacks* are defined as those where the impacts are "moderate to the proper conduct of" hospitals and causes moderate disruptions over a period or affects several wards. This causes limited damage in terms of financial and reputational loss [22]. Moderate severity attacks are secondary infiltration attacks that affects the patients indirectly and has implications for the hospital. This could range from data exposures, breaches to billing systems or attacks on the supply chain [22]. Level 1 or *Low severity attacks* are those where the impacts are "generally limited to the proper conduct of" hospitals and does not usually disrupt organisational processes or in some cases, maybe one ward is impacted [22]. It does not cause any direct patient-harm and are usually tertiary infiltration attacks target the broader hospital infrastructure [23]. Using documented sources for the attack types and severity, the incidents on hospitals can be categorised into these four levels. The framework does not provide specific categorisation for hospitals/CNIs and leaves it to the organisation to decide on how incidents are categorised. Using the guidance from CIRP framework and documented attacks against hospitals and their impact, we have listed the types of attacks against hospitals and their categories.

{Table 1} summaries different types of attacks over the last decade against hospitals, providing details of their effects, security level and real-world examples. For instance, as you can see from the table 1. Distributes Denial of Service (DDoS) attacks represent a hight severity level with the aim of impacting patient care and disruption of critical service. A notable example occurred in 2020 at the University of Vermont Medical Centre, where a DDoS attack disrupted patient appointments and delayed elective procedures, resulting in financial losses of USD 1 million.

<INSERT TABLE 1 HERE>

Impact of cyber-attacks against hospitals go beyond the financial losses. Operational disruptions, compromised patient records, and erosion of trust between healthcare providers and patients are other significant consequences. For example, a ransomware attack on the Los Angeles' Hollywood Presbyterian Medical Centre in 2016 had significant impact not only in both financial and reputational damage, but it impacted workflows and continuum of acute care for patients [24]. [25] showcase how ER nurses were unable to handle patient care at St. Michael Medical Center in Washington requesting emergency services to help them deal with redirecting patients. Patient safety can be threatened due to cyber-attacks especially when it concerns the use of electronic medical devices [26]. Beyond the continuum of care, cyber-attacks have also led to death of patients. Between 2016 and 2021, there has been an estimate of 42-67 deaths of Medicare patients due to system issues caused by ransomware attacks [27]. It is also estimated that the total deaths would surpass this approximation as this does not include patients who have other types of health insurance. Other examples include the cyber-attack against the Massachusetts hospital on Christmas day in 2023 where ambulances were rerouted, patients transferred to other facilities causing significant delays in patient care [28]. Similarly, the UK NHS trusts in London suffered a cyber-

attack on the pathology systems on the 3rd of June 2024. This caused severe disruptions with major trusts such as Kings College Hospitals, Guys's and St. Thomas' NHS foundation and the transplant centres at Harefield Hospital, Royal Brompton and Evelina London Children's Hospital. The damage caused includes several thousand appointments and surgeries being cancelled and impacted GP services causing disruption [29].
Independent of the motive of the perpetrator or the nature of the cyber-attack, cybersecurity function revolves around safeguarding the digital assets of the organisation, to forestall and mitigate the repercussions from cyber-attacks. To be able to do this, a profound understanding of the landscape of malicious attacks evolution in conjunction with emergent technologies is thus needed.

Materials and methods

Overview

This study proposes a multi-method framework for collecting a comprehensive dataset of news articles pertaining to cyber-attacks against hospitals using the GDELT database. GDELT is a database that tracks global news from a wide range of sources, including broadcast, print, and online platforms, spanning over 100 languages. GDELT offers the possibility to collect key individuals, locations, organizations, themes, and events that influence global society. Furthermore, the use of extensive data sources, such as GDELT, is becoming increasingly common in analysing how shifts in news coverage—regarding actors, events, and sentiments [30].
We use NLP, ML and SNA to map interdependencies between the reported events and the entities – in this case, cyber-attacks, and hospitals respectively. Extending the data-driven cyber security (DDCS) approach of [31], a five-step process was adopted to include: data extraction, data scraping, data pre-processing, feature extraction, and social network analysis. While each of these steps are not novel, the combination of these steps into a methodological framework is as this enables healthcare organisations to have a broader picture of the threat landscape. Our methodological framework, which has been applied to cybersecurity in this study, can be replicated in other contexts by modifying the search term selection, time period, and relevant features for further analysis. The process is explained in the following section.

Five-step process

Step1- Data Extraction. This is the first step in the process and comprised four sub-steps. The first sub-step was source identification whereby the selection criteria and the database, GDELT (in our case) was chosen after careful consideration to ensure comprehensiveness and relevance. From the GDELT database, the Uniform Resource Locator (URL) for each of the articles had to be extracted. This was done using a web crawler or a bot that extracted this information in the second sub-step, web crawler configuration. This step included identification of the correct keywords and time period for which the search had to be done. Keywords including "cyber-attack", "information attack", "data attack", "DDos", "DoS", "ransomware", "information security attack", "cyber breach", "information security breach", "data breach", "hospital", "healthcare" were used. The time period was restricted from 2017-2023 to see how the trends in attacks had changed before, during and after COVID-19 pandemic. This sub-step also included pagination which ensures that the web crawler is able to navigate several pages in a systematic manner. This was implemented using the Python library Beautiful Soup that ensured the web crawler iterated through all the pages and extracted date from each of the web pages. creating a date list, navigating the events index page and finally downloading the data by day.
The articles were then grouped by year for longitudinal analysis. Once the GDELT data files were all downloaded, the CSV files were read using the Pandas library. Initially, 1,045,076 articles were downloaded, however, there were several false positives with varied other types of attacks against hospitals or generic cyber-attacks against other sectors. Once the web crawler was configured, the next step was to validate the initial data where checks were done to ensure that only relevant data was going to be used. Those articles that did not pertain to cyber-attacks against hospitals were removed in this sub-step resulting in a total of 39,796 articles. Further actions were taken to filter out articles in English which reduced the total articles to 27,789. The final sub-step in this was metadata collection where a CSV file with 3 columns "URL", "Date" and "Title" were extracted and stored.

Step 2 – Data scraping. This is the second step whereby information from different webpages (from the URLs from step1) can be extracted. For this, we used a library from Python known as Beautiful Soup which enables extraction of information such as the content where the keywords (used in step1) appear in the document (relevant and necessary content for the analysis), organisational names, document title, publication date. This was implemented by fetching the content from each of the web pages through the use of requests library. This resulted in the content being retrieved in HTML (Hypertext Markup Language) format. After this, a Beautiful Soup object in Python was created that enabled us to parse the HTML structure. Specific information was extracted through the use of functions such as "find and find_all" especially for scanning the text within the HTML data and to filter the lines that contained any/all of the keywords. This approach enabled us to obtain and organise all necessary data that will be used in the next steps for analysis and all relevant information from the articles extracted were captured. To the existing CSV file, a new column "Context" was created to store the actual news content. To avoid issues with the scraping, a 10-second timeout was established and sites that were non-responsive returned a NAN in the context column. This was also particularly useful as a robust error handling mechanism to manage issues like CAPTCHA, dynamic content loading, and access restrictions.

Step 3 – Data pre-processing. This is the third step in which we checked if the data obtained from the first two steps are consistent and can be used. This included data cleaning whereby inconsistencies and issues with missing data were dealt with. For example, in some cases, the context column comprised records that were not consistent due to several reasons such as unresponsive websites, broken links, issues with CAPTCHA, dynamic content or access restricted sites having NAN in this column. The next step of the pre-processing included identifying non-English character sets and unintelligible data in this column. These were identified and removed in this step. . Furthermore, duplicated records were also removed resulting in a total of 18,009 articles that mentioned 18,009 different attacks against hospitals.

Step 4 – Feature extraction. This is the fourth step in which five attributes were obtained from the news articles in this step namely type of cyber-attack, severity level, hospital name, hospital type and whether the hospital was private or public. Several NLP techniques, including tokenization, lower case conversion, stop word removal, and lemmatization were employed [32] to extract cyber-attack keywords present in the articles. Tokenization is a process where sentences in an article are now separated. This step is crucial as it splits the article into smaller tokens that can be used in the analysis later. The next step is converting all the tokens into lower case, and this is done to ensure that any comparisons of the data is accurate. The third part of the process is stop-word removal which removes frequently occurring text such as prepositions and articles. Then lemmatization process is applied whereby a morphological analysis and vocabulary is used to clearly identify the base form of words to identify those words that would carry a common base word. For example, words such as studies or studying would have the common base word "study". Once these steps were completed, SpaCY, the Python library was used for Named Entity Recognition (NER). This involves parsing the text to extract relevant entities and categorise them appropriately. For example, we identify and extract hospital names, types of cyber-attacks, and severity levels. The types and severity of cyber-attacks were based on the literature mentioned in the previous section. All names of hospitals were extracted and finally, hospital types were defined by using a list of predefined keywords from the literature to include rural hospitals, teaching hospitals, clinics etc. [33]. This step provided a list of 18,073 hospitals over the 6-year period that have suffered a cyber cyber-attack.
{Table 2} shows a sample of the final dataset that we collected, reporting information about (i) the link to the news discussing the cyber-attack;(ii) the date the news was published; (iii) the title of the news; (iv) a brief summary of the incident; (v) the type of the cyber-attack; (vi) the level of severity of the attack; (vii) the targeted hospital; (viii) the type of the hospital; and (ix) whether the hospital is public or private. This systematic approach ensures that the data is accurately categorised and prepared for identifying trends and patterns in cyber-attacks against hospitals.

<INSERT TABLE 2 HERE>

Step 5 – SNA. This is the final step in the process where we used social network analysis. SNA is a set of tools and techniques used to explain how social entities are connected and interact with one other. It focuses on

relationships and enables us to understand how the patterns of relationships can be used to map the evolving cyber threat landscape. We created a bipartite network contains two different sets of nodes [34]. One set represents the hospitals, and the other set represents the types of cyber-attacks. The edges represent the relationships that exist between the sets of nodes. In this context, an edge connects a hospital to a cyber-attack if for instance, a particular hospital has experienced a specific type of cyber-attack. In other words, the edge between the node represents the occurrence of a particular type of cyberattack at a specific hospital by year. Using this structure is beneficial as it provides insights into the relationships between hospitals and cyber-attacks. Attributes such as the types of hospitals, severity levels and country are added to the data. In order to identify the most important nodes within the network, we employed the degree centrality measure [34], which is the number of cyber-attacks against hospitals, and for the cyber-attack is the number of hospitals that cyber-attack was targeting at. A higher degree centrality for a cyber-attack indicates that it is more widespread and has affected a larger number of hospitals. This can help identify the most common or pervasive types of cyber-attacks in the healthcare sector. Temporal analysis is also conducted to observe how the network evolves over time, providing insights into trends and shifts in the cyber threat landscape. We used the NetworkX python library.

{Figure 1} illustrates the five-step process. Elongated circles indicate that start (data extraction) and the end of the process (social network analysis). Rectangles show the actions, while diamonds show decision that must be adopted. Links using arrow to indicate the flow of the process.

<INSERT FIGURE 1 HERE>

Results

The trend in the number of articles from 2017-2023 from the 18009 attacks that had reported between by year is given in {Figure 2}.

<INSERT FIGURE 2 HERE>

{Table 3} provides a breakdown of cyber-attacks from 2017 to 2023, categorised by their severity levels. It indicates that compared to the 1987 attacks reported in 2017, 2023 had a 72% increase in the number of cyber-attacks against hospitals accounting for 3416 attacks. Classifying these attacks based on the severity level also showed that there is a huge increase in the number of critical (Level 4) attacks over the years. 2017 saw a total of 1116 attacks that were critical while 2023 had 3123 critical attacks, an increase by 179. This indicates an overall increase in the number of cyber-attacks over the years, with a notable rise in critical severity attacks. Ransomware and advanced persistent threats (APT) were classified as critical, while DDoS, MITM were classified as high severity, DoS, Phishing, Password Attacks, SQL injections were moderate attacks and attacks such as the DNS attacks or URL interpretation were classified as low based on the literature [23].

<INSERT TABLE 3 HERE>

{Figure 3} shows the distribution of cyber-attacks across 2898 hospitals during the COVID -19 pandemic (2020). The blue triangles at the right side of {Figure 4} represent the different types of cyber-attacks. Ransomware, Cyber espionage, cyber terrorism, DDos and MITM are the most frequent types of cyber- attacks targeting hospitals. The red dots at the left side represent the hospitals. The grey lines represent the relationships between hospitals and types of cyber-attacks indicating which type of attack targets a specific hospital.

<INSERT FIGURE 3 HERE>

Finally, to understand how the threat landscape has evolved, centrality measure of degree was calculated to identify the attacks that most hospitals suffered over time. {Table 4} reports a detailed overview of various cyber-attacks over the years by using the degree centrality, indicating the prominence of each type of attack

within the data. Compared to the 2017, where phishing had the highest degree centrality value at 4.690, indicating it was the most significant attack type that year; the 2023 the situation had changed considerably. APT (Advanced Persistent Threats) had the highest degree centrality value at 6.873, showing its critical importance. Ransomware also became much more significant, with a degree centrality value of 6.452. DDoS attacks were also prominent, with a value of 3.976. Interestingly, phishing, which was the most significant attack in 2017, had a much lower degree centrality value of 0.645 in 2023, indicating a relative decrease in its prominence compared to other attack types. Overall, the data shows a shift from phishing being the most significant threat in 2017 to APTs and ransomware becoming the most critical threats by 2023. This shift highlights the increasing complexity and sophistication of cyber-attacks over the years. The rise in the prominence of APTs and ransomware suggests that attackers are focusing more on persistent and highly damaging attacks, reflecting the evolving strategies in the cyber threat landscape.

<INSERT TABLE 4 HERE>

Looking at the attributes obtained from the feature extraction, teaching hospitals, public hospitals and academic medical centres are more prone to Level 4 and Level 3 attacks including cyber terrorism/state actor-sponsored criminal activities, APTs, DDoS while community hospitals, children's hospitals, clinics are more prone to Level 1 and Level 2 attacks.

Discussion

This study offers a novel methodological approach for collecting and analysing different types of cyber-attacks against hospitals. It maps the relationship between attacks and hospitals, identifies various types of attacks and distinguish the most prominent attacks affecting hospitals over time. The healthcare sector has experienced an increasing number of attacks as we shown in our findings. This is because hospitals serve as vital components of a country's healthcare infrastructure, managing sensitive patient data, medical records, and essential services. Consequently, they become prime targets for cybercriminals, state-sponsored actors, and hacktivists due to the valuable information they hold, including patient health records, research data, and intellectual property [37].
In analysing attack pattern, we found two distinct trends. Level 1 attacks such as phishing attacks, DoS attacks or SQL injections have decreased due to improved preparedness, including implementation of multi-factor authentication and regular audits [3]. This is aligned with the recent literature that shows that hospitals have increased their cybersecurity capabilities and the familiarity with and constant threat monitoring for phishing tactics can be attributed to decrease in the number of phishing attacks [41]. Another study [42] also showcases that hospitals' preparedness have increased as most hospital organisations now implement preventative measures such as multi-factor authentication (MFA) and conduct regular audits which lead to effectively deterring low level attacks such as SQL injections or DoS attacks despite these remaining a threat. However, we observed that Level 3 and 4 attacks are rising, with public hospitals and academic medical centres being particularly vulnerable to ransomware and cyber terrorism. This is also aligned with a recent study that emphasis an increase of ransomware attacks as hospitals lack adequate training in cybersecurity awareness and best practices, creating vulnerabilities that attackers can exploit [47]. Indeed, since 2020, there has been a significant increase in critical attacks such as cyber espionage, state-sponsored attacks which were not much prevalent prior to COVID. Specifically, these two hidden threats were more frequent as there were further benefits for the threat actor such as intellectual property theft and getting an oversight of intelligence operations [35]. Similarly, state-sponsored attacks especially from hacker groups in North Korea, China and Russia were operating covertly in the cyberspace to evade political responsibilities [36,38]. Moreover, nation-states may target healthcare institutions for geopolitical reasons,

leading to cyberterrorism, espionage, and other state-sponsored criminal activities that can compromise national security [39, 40].

Despite regulatory requirements like medical device regulations (MDR), Good Clinical Practice (GCP) and the General Data Protection Regulation (GDPR) many healthcare organisations remain reluctant to disclose incidents, leading to substantial fines – with in EU, there have been 163 fines issued due to non-compliance with the GDPR against healthcare organisations accounting for 16 million euros [3]. Indeed, as pointed out in the ENISA report [3], most healthcare organisations rely hugely on incidents that are publicly disclosed by the victim organisations and are thus dependent on deliberate disclosures or sometimes through unintentional data leaks.

To this end, our multi-method framework enhances pattern identification for organisational-level policy makers while automating security data gathering. Using the proposed methodological framework enables better pattern identification that cyber policy makers at the organisational level can use to summarise huge volumes of information to obtain actionable intelligence. This also helps organisations automate security data gathering, thereby minimising manual effort which then paves way for cybersecurity professionals to focus on strategic tasks. This is especially important as studies [45] show that many hospital organisations, especially in times of economic downturn have reduced investments in health workforce and investments in technologies and implement absorptive capacity policies which focus only on critical hospital functions. Hence, cybersecurity professionals will not have the luxury of large teams and will need to prioritise tasks effectively. They must identify and address the most critical threats first, ensuring that limited resources are used efficiently to maintain robust security postures.
Integration of advanced ML, NLP, and SNA methods for data collection will provide a better understanding of the dynamic threat landscape which can enhance cybersecurity standards such as ISO 27000 series and IEC62442 and policy development. Indeed, the need to use and integrate advanced methodology is also emphasised by a recent study [43] that shows the importance of supporting real-time data analysis risk assessment and decision-making processes. More specifically, a robust methodological framework such as the one we propose will enable enhanced threat detection and response, better risk assessments and pave way for data-driven decision-making. Our multi-method framework has the capability to analyse huge volumes of real-time data and thereby identify patterns to detect anomalies that could indicate emerging threats. For instance, while phishing attacks are still common and talked about, our real-time data showcases that the number of successful attacks that have been reported based on the impact has reduced while advanced persistent threats and critical attacks have increased. Understanding these trends are pivotal as this capability will allow development of cybersecurity policies and standards that are robust and will also allow for adaptive and proactive threat detection and cyber response [44]. Similarly, using the multi-method framework and adding predictive capabilities can enable policy makers to accurately predict potential threats and refine risk assessment methodologies and standards to ensure they are effective and relevant in the evolving threat landscape. This enables cybersecurity professionals to better prepare for a response by dynamically allocating resources to counter the risks.

Limitations and future work

This study provides a methodological framework for extracting real-time data to map cyber threat in the healthcare sector. While there are studies that quantitatively specify types of attacks [11,12,21], they relied on voluntarily disclosed data. There have not been many studies that employ multi-method approach including Machine Learning, NLP and SNA and use real data from conventional and unconventional signals – GDELT- to investigate and map the current types of attacks against the sector. There are few limitations to this study. Firstly, we applied SNA by using centrality measure of degree to evaluate the most prevalent attacks, future research could combine network measures with hospitals attribute (countries, performance indicators, size) to analyse if hospital that occupy central position in the network are more prone to experiencing state-sponsored attacks. Along the same lines, network models can be applied to observe how the network evolves overtime. Secondly, we used longitudinal data to showcase how the severity of threats has changed overtime, but we have not used any predictive models. Future researchers could incorporate predictive modelling using methods: GCN or Node2Vec based on the historic data available. Being able to predict future events with high precision will certainly help healthcare organisations to not only understand the current landscape, but also improve their preparedness for such events.

Conclusion

This study is important as it developed a framework for and implemented a multi-method approach for collecting real-time data from several sources, identifying patterns and relationships between attacks and hospitals and exploring the current cyber-attack trends in healthcare sector. The results show that there is an exponential growth in high and critical attacks, while low severity attack diminishes overtime. The approach presented in this study allows healthcare institutions to identify potential vulnerabilities, anticipate threats, and implement proactive measures to mitigate risks. Furthermore, it enables them to prioritise resources effectively, focusing on areas of highest risk or potential impact. As the frequency of severity of attacks tend to increase, understanding the threat landscape is a fundamental step in safeguarding this critical infrastructure.

Acknowledgements

NA

Authorship confirmation/contribution statement

Author 1: Conceptualisation (lead), funding acquisition (lead), Writing – original draft (lead), writing – review and editing (equal contribution), methodology (support), software (support)
Author 2: Conceptualisation (support), visualisation (lead), methodology (lead), software (lead)

Authors disclosure statement

The authors have no competing interests to declare that are relevant to the content of this article.

Funding statement

The authors wish to acknowledge funding received by Networks and Urban Systems Centre -NUSC- from the University of Greenwich (2022-2023).

References

[1] National Cyber Security Centre (UK). Case study: Securing Critical National Infrastructure [Internet]. Annual Review 2023. London: National Cyber Security Centre (UK); 2023 Nov 14 [cited 2024 Feb 12]. Available from: https://www.ncsc.gov.uk/collection/annual-review-2023/resilience/case-study-securing-cni

[2] National Cyber Security Centre (UK). NCSC warns enduring significant threat to UK's critical infrastructure [Internet]. London: National Cyber Security Centre (UK); 2024 Feb 5 [cited 2024 Feb 12]. Available from: https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure

[3] European Union Agency for Cybersecurity (ENISA). Checking up on health: Ransomware accounts for 54% of cybersecurity threats [Internet]. ENISA; 2023 Jul 5 [cited 2024 Feb 12]. Available from: https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats

[4] Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research*. 2018 May 28;20(5):e10059.

[5] Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*. 2020 Dec;20:1-0.

[6] Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*. 2022 Aug 11;4:862221.

[7] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*. 2017 Jan 1;25(1):1-0.

[8] British Computer Society (BCS). Biggest healthcare cyber-attacks this decade [Internet]. BCS; 2023 Jan 9 [cited 2024 Feb 12]. Available from: https://www.bcs.org/articles-opinion-and-research/biggest-healthcare-cyber-attacks-this-decade/

[9] The New York Times. Cyberattack on a German Hospital Leads to Death of Patient [Internet]. New York Times; 2020 Sep 18 [cited 2024 Feb 12]. Available from: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

[10] National Security Agency (NSA). Science of Security [Internet]. National Security Agency (NSA); [cited 2024 Feb 12]. Available from: https://www.nsa.gov/what-we-do/research/science-of-security/

[11] Bakdash JZ, Hutchinson S, Zaroukian EG, Marusich LR, Thirumuruganathan S, Sample C, Hoffman B, Das G. Malware in the future? Forecasting of analyst detection of cyber events. *Journal of Cybersecurity*. 2018;4(1):tyy007.

[12] Bobowska B, Choras M, Wozniak M. Advanced Analysis of Data Streams for Critical Infrastructures Protection and Cybersecurity. J. Univers. Comput. Sci.. 2018 Jan 1;24(5):622-33.

[13] Sun N, Zhang J, Rimba P, Gao S, Zhang LY, Xiang Y. Data-driven cybersecurity incident prediction: A survey. IEEE communications surveys & tutorials. 2018 Dec 7;21(2):1744-72.

[14] Galla D, Burke J. Predicting social unrest using GDELT. In International conference on machine learning and data mining in pattern recognition 2018 Jul 8 (pp. 103-116). *Cham: Springer International Publishing*.

[15] Yonamine JE. Predicting future levels of violence in afghanistan districts using gdelt. Unpublished manuscript. 2013.

[16] Jakel T. Using Sentiment Data from the Global Database for Events, Language and Tone (GDELT) to Predict Short-Term Stock Price Developments (Bachelor's thesis, *University of Twente*).

[17] Kwon J, Johnson ME. Proactive versus reactive security investments in the healthcare sector. Mis Quarterly. 2014 Jun 1;38(2):451-A3.

[18] Ayala L, Ayala L. Medical Facility Cyber-Physical Attacks. *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*. 2016:39-45.

[19] Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E, Kim B, King A, Mullen-Fortino M, Park S, Roederer A, Venkatasubramanian KK. Challenges and research directions in medical cyber–physical systems. *Proceedings of the IEEE*. 2011 Oct 18;100(1):75-90.

[20] Coventry L, Branley D. *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward*. Maturitas. 2018 Jul 1;113:48-52.

[21] He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of medical Internet research*. 2021 Apr 20;23(4):e21747.

[22] The Scottish Government. Introduction to the Cyber Incident Response Plan (CIRP) [Internet] Scottish Government; 2020 Sep 18 [cited 2024 Jun 12]. Available from: https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2019/10/cyber-resilience-incident-management/documents/cyber-incident-response-plan---private-and-third-sector-template/cyber-incident-response-plan---private-and-third-sector-template/govscot%3Adocument/Cyber%2BCapability%2BToolkit%2B-%2BCyber%2BIncident%2BResponse%2B-%2BCyber%2BIncident%2BResponse%2BPlan%2B%2528CIRP%2529%2Bv1.2.docx

[23] Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC medical informatics and decision making*. 2019 Dec;19(1):1-1.

[24] van Boven LS, Kusters RW, Tin D, van Osch FH, De Cauwer H, Ketelings L, Rao M, Dameff C, Barten DG. Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. Annals of emergency medicine. 2024 Jan 1;83(1):46-56.

[25] Neprash HT, McGlave CC, Rydberg K, Henning-Smith C. What happens to rural hospitals during a ransomware attack? Evidence from Medicare data. The Journal of Rural Health. 2024 Mar 17.

[26] Alhammad A, Yusof MM, Jambari DI. A Review of Cyber Threats to Medical Devices Integration with Electronic Medical Records. In2022 International Conference on Cyber Resilience (ICCR) 2022 Oct 6 (pp. 1-6). IEEE.

[27] McGlave CC, Neprash H, Nikpay S. Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients. The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023). 2023 Oct 4.

[28] The Record. Cyberattack on Massachusetts hospital disrupted records system, emergency services [Internet]. The Record; 2023 Dec 29 [Cited 2024 Jun 06]. Available from: https://therecord.media/cyberattack-on-massachusetts-hospital-disrupted-health-record-system

[29] digital Health. NHS issues urgent call for O-type blood donors following London cyber attack [Internet]. digital Health; 2024 Jun 10 [Cited 2024 Jun 20]. Available from: https://www.digitalhealth.net/2024/06/nhs-issues-urgent-call-for-o-type-blood-donors-following-london-cyber-attack/#:~:text=The%20cyber%20attack%20on%20pathology,and%20the%20Evelina%20London%20Children's

[30] Buckingham K, Brandt J, Anderson W, do Amaral LF, Singh R. The untapped potential of mining news media events for understanding environmental change. *Current Opinion in Environmental Sustainability*. 2020 Aug 1;45:92-9.

[31] Coulter R, Han QL, Pan L, Zhang J, Xiang Y. Data-driven cyber security in perspective—Intelligent traffic analysis. *IEEE transactions on cybernetics.* 2019 Oct 16;50(7):3081-93.

[32] Pant VK, Sharma R, Kundu S. An overview of Stemming and Lemmatization Techniques. Advances in Networks, Intelligence and Computing.:308-21.

[33] Gallagher Healthcare. What are the Different Types of Hospitals? [Internet]. Gallagher Healthcare; 2018 Mar 3 [cited 2024 Feb 12]. Available from: https://www.gallaghermalpractice.com/blog/post/what-are-the-different-types-of-hospitals

[34] Everett MG, Borgatti SP. Extending centrality. Models and methods in social network analysis. 2005 Feb 7;35(1):57-76.

[35] Tokat Y. Cyber Threats to Hospitals and Critical Infrastructure in Times of COVID-19 Pandemic. Available at SSRN 4539458. 2021 Jul.

[36] Wiggen J. Impact of COVID-19 on cyber crime and state-sponsored cyber activities. Konrad-Adenauer-Stiftung; 2020 Jun.

[37] Ahmed NB, Daclin N, Olivaux M, Dusserre G. Cybersecurity challenges for field hospitals: impacts of emergency cyberthreats during emergency situations. International Journal of Emergency Management. 2023;18(3):274-92.

[38] Wilner AS, Luce H, Ouellet E, Williams O, Costa N. From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. International Journal. 2021 Dec;76(4):522-43.

[39] UK Government. UK Coronavirus (COVID-19) alert level increased from level 3 to level 4 [Internet]. UK Government; 2021 Dec 12 [cited 2024 Feb 12]. Available from: https://www.gov.uk/government/news/uk-coronavirus-covid-19-alert-level-increased-from-level-3-to-level-4

[40] UK Government. National Cyber Security Strategy 2022 [Internet]. UK Government; [updated 2022 Dec 15; cited 2024 Feb 12]. Available from: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[41] Vanderbilt University Medical Centre 2024 [Internet]. VUMC News; 2024 Jun 5 [cited 2024 Dec 18]. Available from: https://news.vumc.org/2024/06/05/phishing-attacks-are-targeting-the-health-care-industry-some-tactic-to-familiarize-yourself-with/

[42] HIPAA Journal. Healthcare data breaches due to phishing. 2024 Jan 6 [cited 2024 Dec 18]. Available from: https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/

[43] Radanliev P, De Roure D. Disease X vaccine production and supply chains: risk assessing healthcare systems operating with artificial intelligence and industry 4.0. Health and Technology. 2023 Jan;13(1):11-5.

[44] Forbes. Closing the gaps in Security through AI and ML Forbes Magazine 2022 Feb 14 [cited 2024 Dec 18]. Available from Closing The Gaps In Security Through AI And ML

[45] Foroughi Z, Ebrahimi P, Aryankhesal A, Maleki M, Yazdani S. Hospitals during economic crisis: a systematic review based on resilience system capacities framework. BMC Health Services Research. 2022 Jul 30;22(1):977.

[46] Radanliev P. Dance as a mental health therapy in the Metaverse: exploring the therapeutic potential of Dance Movement Therapy as a non-pharmacological treatment in the Metaverse. Frontiers in Computer Science. 2024 Feb 7;6:1334027.

[47] Saira, G., Arvind, S., Mike, D. Cyber-attacks are a permanent and substantial threat to health systems: education must reflect that. Digital health, 8 (2022): 20552076221104665.

Tables

Attacks against hospitals

Attack	Effect	Severity	Example and impact
DDoS[a]	Loss of critical services, impact on patient care	High	In 2020, the University of Vermont Medical Centre suffered a DDoS attack, affecting patient appointments and delaying elective procedures. Financial loss: USD[b] 1 million [5].
Ransomware	Data loss, operational disruption	Critical	The WannaCry attack in 2017 paralyzed the United Kingdom's NHS[c], delaying treatment plans and rerouting ambulances. Financial impact: the attack costed the NHS over 92 million GBP[d] [21]. Patient impact: Over 19000 appointments were cancelled [21] and 34 % of the NHS trusts were disrupted [22].

[a] Distributed Denial of Service
[b] United States Dollar
[c] National Health Scheme
[d] Great Britain Pound

Phishing	Unauthorized access to sensitive data	Moderate	In 2021, Finnish psychotherapy centre Vastaamo faced a phishing breach, exposing patient therapy records. Patients received ransom emails demanding [23] EUR[e] 200 in bitcoin payment to not expose discussions with therapist to become public. Reputation damage: Loss of trust. Patient impact: Mental distress for patients who sought victim support services.
Insider Threats	Unauthorized data access, sabotage	Moderate	In 2022, a previous staff member of BayCare Health System in Florida illicitly accessed patient records of 193,947 patients, resulting in the possible exposure of protected health information (PHI). The breach was attributed to tracking pixels utilized by Advocate Aurora Health, a partnering company. These tracking pixels, typically utilized for targeted marketing and monitoring visitor activity, inadvertently revealed information about patient engagements with BayCare Clinic's patient portal. Reputation damage: loss of trust and further scrutiny from public, regulatory authorities. Financial Loss: class action against the company [24]. Patient impact: Loss of privacy
IoT Vulnerabilities	Patient safety risks, data exposure	Moderate	In 2023, Medtronic's insulin pumps were found vulnerable to remote attacks whereby the attacker can alter insulin dosage to the patients from an adjacent network. Patient safety: Risk of insulin overdose [25].
AI-based Attacks	Misdiagnoses, compromised treatment recommendations	Moderate	AI-driven diagnostic tools may be intentionally manipulated, leading to incorrect diagnoses. These could be due to the limitations of the AI tool which exacerbate existing disparities and provide biased results [26]. Impact on patient care: Delayed or incorrect treatment.
Robotic Surgery Vulnerabilities	Surgical errors, patient harm	High	In 2022, a group of researchers simulated cybersecurity attacks that could potentially disrupt a robotic-assisted surgery, resulting in unintended incisions. Patient safety: Surgical errors can result in bleeding, infection, and other adverse outcomes [27].
Wearable Device Exploits	Unauthorized data access, privacy breaches	Moderate	61 million records of individuals containing sensitive health data were inadvertently leaked from an unsecured database from the company GetHealth. Patient safety: Exposure of personal health information breaching privacy and potential harm if data is tampered with [28].
Man in the middle (MITM)	Intercepting sensitive data and/or compromise patient care.	High	In 2015, UCLA[f] Health System experienced a breach from MITM attack, which resulted in the theft of patient data and the compromise of 4.5 million patients [29].

Table 1: Example of attacks against hospitals in the last decade

Sample of final dataset

URL	Date	Title	Context	Attacks	Hospital Names	Hospital Types	Public/Private	Severity Level
https://www.digitalhealth.net/2017/01/update-trojan-malware-blamed-for-barts-cyber-attack-2/	12/12/2017	NHS Trusts vulnerable to cyber attack due to irregular app testing	England's biggest NHS trust says malware was behind a cyber-attack	Ransomware	['Newham University Hospital']	['Teaching Hospital']	['Private Hospitals']	Level 4

[e] Euro
[f] University of California, Los Angeles

			that forced the trust to shut down some IT systems for four days.					

Table 2: Sample of the final dataset

Severity of attacks by year

Severity level	2017	2018	2019	2020	2021	2022	2023
Level 4 - Critical	1116	1252	1256	1988	2583	2609	3123
Level 3- High	738	750	757	432	98	116	209
Level 2 - Moderate	79	89	121	188	63	98	101
Level 1 - Low	54	52	55	80	10	9	17
Total	1987	2143	2189	2688	2754	2832	3416

Table 3: Attacks by severity

Top 4 attacks by degree centrality by years

Attack	Year	Degree centrality Value (normalised)
Phishing	2017	4.690
Password Attack	2017	1.250
SQL injections	2017	0.563
DNS	2017	0.438
Ransomware	**2017**	**0.188**
Phishing	2018	4.592
DoS[g]	2018	2.095
MITM[h]	2018	0.905
SQL[i]	2018	0.619
Ransomware	**2018**	**0.381**
Social Engineering	2019	2.988
DDoS[j]	2019	1.876
Ransomware	**2019**	**1.451**
Password attack	2019	0.976
Phishing	2019	4.312
Ransomware	**2020**	**3.928**
Cyber espionage	2020	3.703
Cyber terrorism / state actors	2020	3.561
DDoS	2020	2.175
MITM	2020	1.295
Cyber terrorism / State actors	2021	4.373
Ransomware	**2021**	**4.194**
APT	2021	3.200
Phishing	2021	1.329
DoS	2021	1.311
Ransomware	**2022**	**5.386**
APT[k]	2022	3.876
DDoS	2022	2.762

[g] Denial of Service
[h] Man-in-the-middle
[i] Structured query language
[j] Distributed Denial of Service
[k] Advanced persistent threat

DoS	2022	1.843
MITM	2022	0.990
APT	2023	6.873
Ransomware	**2023**	**6.452**
DDoS	2023	3.976
MITM	2023	0.972
Phishing	2023	0.645

Table 4: Top 5 attacks from 2017-2023 by degree centrality