sustainability

Article

Epistemological and Bibliometric Analysis of Ethics and Shared Responsibility—Health Policy and IoT Systems

Petar Radanliev * **and David De Roure**

Oxford E-Research Centre, Engineering Sciences Department, The University of Oxford, 7 Keble Rd, Oxford OX1 3QG, UK; radanliev@yahoo.com

* Correspondence: petar.radanliev@oerc.ox.ac.uk

Abstract: The focus in this paper is placed on shared responsibility and ethics in health policy, specific to Internet of Things (IoT) devices in healthcare systems. The article assesses how the introduction of IoT brings risks to the security of medical systems. The justification for this research emerges from the opportunities emerging from digital technologies for medical services, but also creating a range of new cyber risks in the shared healthcare infrastructure. Such concerns are often not visible to individual departments in an integrated healthcare system. In addition, many healthcare organisations do not possess cyber skills and are faced with barriers to the adoption of smart manufacturing technologies, e.g., cost. These barriers trigger ethical concerns related to responsibility of cyber risks in shared healthcare systems.

Keywords: bibliometric analysis; COVID-19 and healthcare systems; ethics of shared risk; internet-of-things and cyber risk

Citation: Radanliev, P.; De Roure, D. Epistemological and Bibliometric Analysis of Ethics and Shared Responsibility—Health Policy and IoT Systems. *Sustainability* **2021**, *13*, 8355. https://doi.org/10.3390/su13158355

Academic Editor: Gwanggil Jeon

Received: 17 June 2021
Accepted: 26 July 2021
Published: 27 July 2021

1. Introduction

This article conducts an epistemological and bibliometric analysis of shared responsibility and ethics, specific for cybersecurity policy of IoT devices and systems in healthcare. Present applications of IoT devices in the medical field include wearables (e.g., Apple Watch), wirelessly connected devices (e.g., like blood pressure and heart rate monitoring cuffs, glucometer), and sensors for remote monitoring and management that benefit patients, families, physicians, hospitals, and insurance companies. The advancement of IoT devices in the medical field spans into monitoring managing extremely challenging illnesses, such as Parkinson's disease monitoring or depression and mood monitoring and includes some of the most advanced methods in the medical field, such as ingestible sensors and connected inhalers. This presents opportunities for remote monitoring and management of exceptionally challenging diseases and illnesses, which brings the focus of IoT devices in monitoring and managing future waves of the COVID-19 pandemic.

The aim is to use knowledge from COVID-19 to construct solutions for a digital health policy in a future Disease X event. Considering the need for periodic revision, in this study, we use research records on ethics of shared responsibilities established prior to the emergence of COVID-19 to extract knowledge, but we distinguish between the time periods with a bibliometric analysis, literature review and a case study. In the bibliometric analysis, we reviewed the ethical research on shared responsibility of IoT systems. Secondly, we analysed recent studies on IoT and cyber risk. Then, we used epistemological approach to relate that knowledge to ethics, shared responsibility, health policy, and IoT. Then, we advance the earlier work on the ethical sharing of risk responsibilities, with a new design for ethical awareness, transparency, and accountability, with a specific focus on ethics in assessing the shared risk in IoT-enabled digital healthcare systems.

2. Bibliometric Analysis with Statistical Software

The statistical software used for bibliometric analysis builds upon recent research on 'data mining and analysis of scientific research data records on COVID-19 mortality, immunity, and vaccine development' [1], with a specific focus on IoT, cyber risk, and ethics in health policy for shared responsibilities. In other words, for the bibliometric analysis, we used the 'bibliometix' package [2] and the VOSviewer computer program [3]. Since Google scholar and other search engines were used excessively in the literature review, we searched for records on the Web of Science Core Collection. Our search for scientific literature on the topics, 'Internet of Things, AND ethics, AND cyber risk', produced only one record. Our second search included the same search parameters, we only replaced 'risk' with 'security'; this resulted with only two records. In our third search, we kept only 'Internet of Things, AND ethics'. This produced 88 records, which enabled us to perform a bibliometric review and to seek concepts related to ethics, shared responsibility, health policy, and IoT through graphical visualisation and categorisations of data records—see Figure 1.

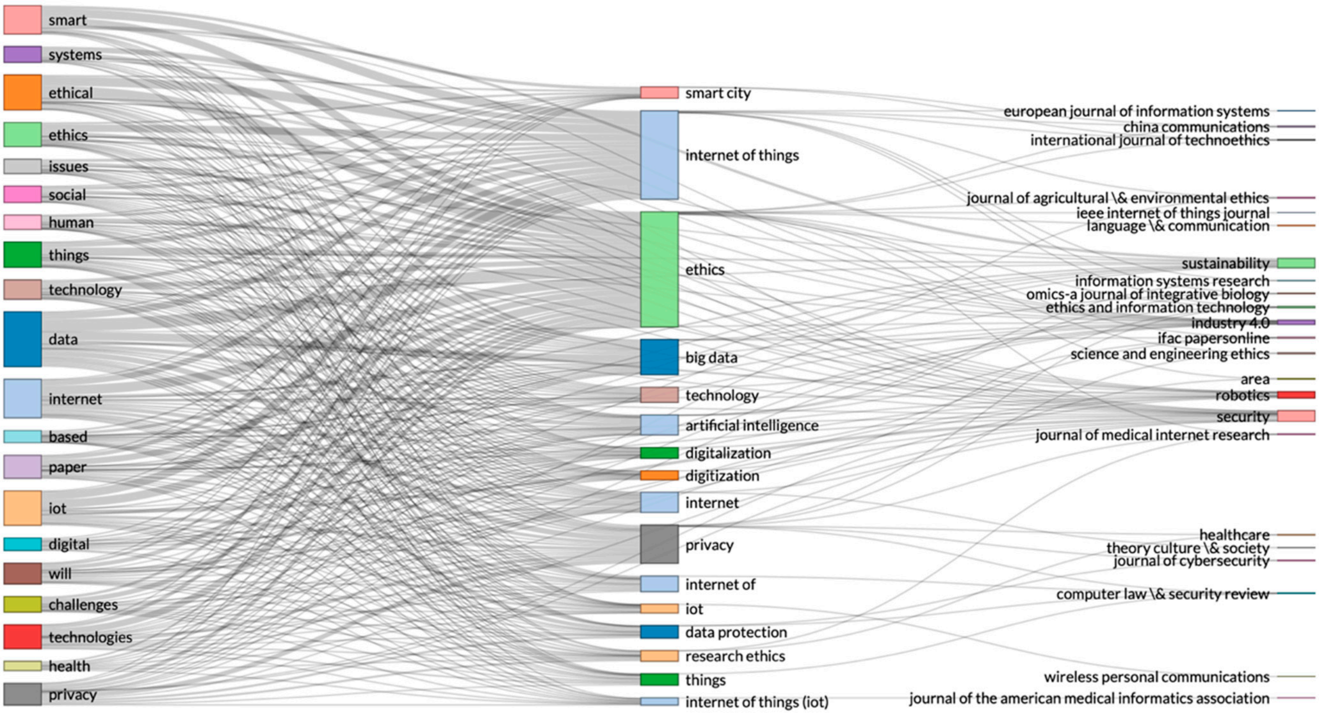

Figure 1. Bibliometric analysis—three-fields plot: keywords from abstracts on the left, keywords from the texts in the middle, and journal sources on the right.

From the three-fields plot in Figure 1, we can see that in the data records on 'Internet of Things, AND ethics', the topics of shared responsibility and health policy are not represented. The only related category is healthcare. From the abstract and article keywords, extracted by the 'bibliometrix' package, the topics of privacy, data protection, and risk are of relevance to health policy and IoT. In addition, the topics on ethical awareness, transparency, and accountability are missing. To analyse this data record with a different bibliometric approach, we used factorial analysis in Figure 2.

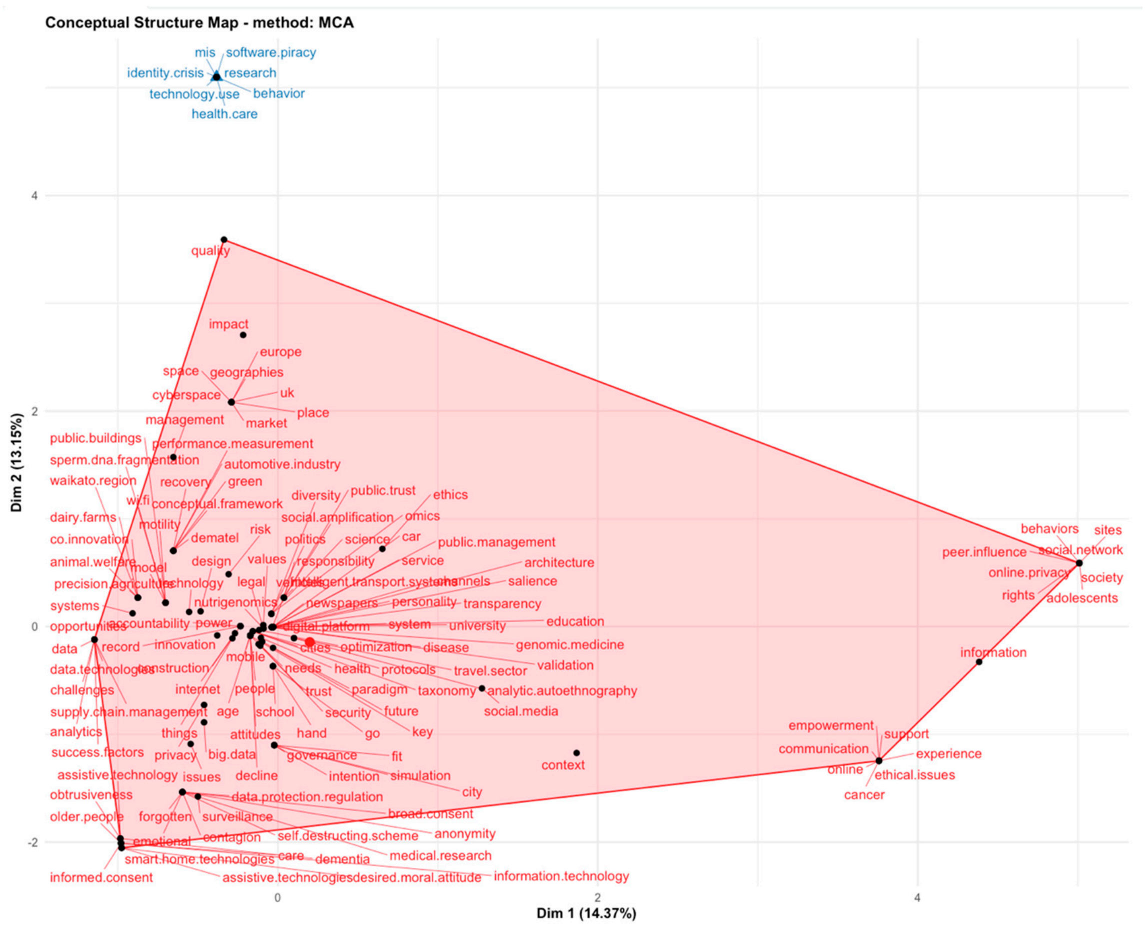

Figure 2. Bibliometric conceptual structure map—factorial analysis.

From the factorial analysis in Figure 2, we can see the topics investigated in different research clusters. Although there is no clear connection between the topics researched in this study, we can see the keywords medicine, medical research, and care, which signifies that although there are no related research studies at present, the research community is actively looking at these topics in combination with IoT, new technologies, cyber-risk, and ethics.

A separate search on 'Internet of Things, AND cyber risk' produced 192 records. We designed a three-fields plot (in Figure 3) and we can see a very strong interconnection in the research on IoT and cyber risk, but the keywords related to shared responsibility in health policy are still missing.

We designed an alternative three-fields plot (in Figure 4) and separated the field by journal sources, keywords from articles, and most relevant publications (chosen by the R 'bibliometrix' package). Since this data record was on IoT and cyber risk, we were trying to find reference and some connection to health policy. The closest we found was 'healthcare' (see Figure 4).

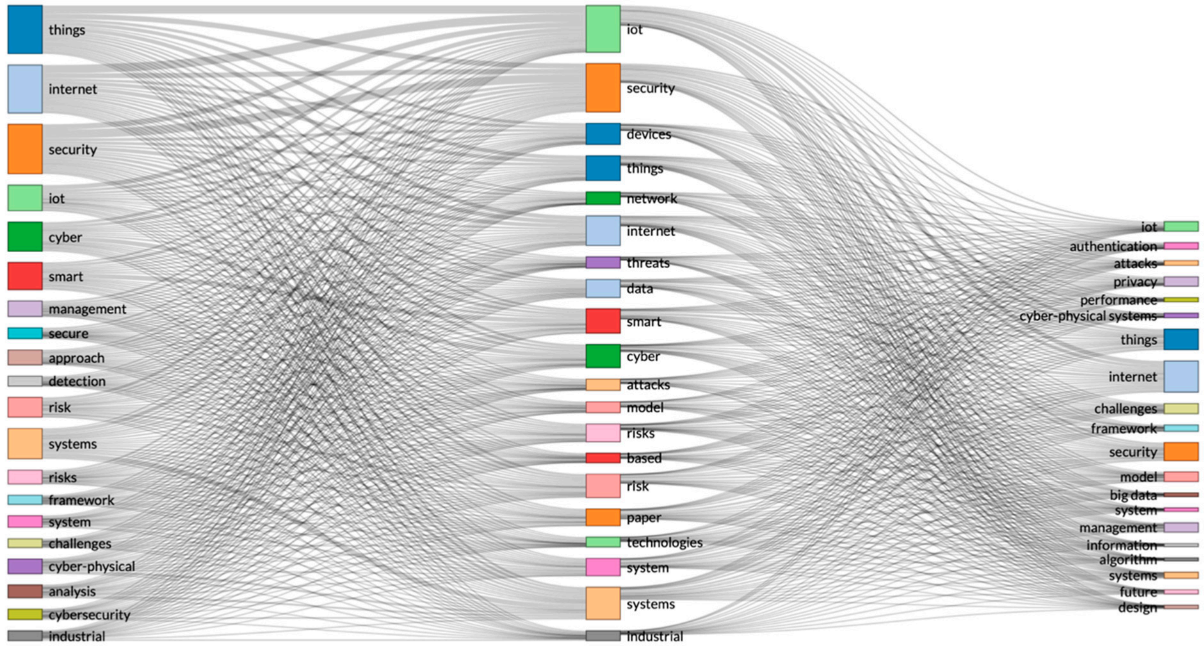

Figure 3. Bibliometric analysis—three-fields plot: keywords from abstract in the middle, keywords from the titles on the right, keywords from the texts in all articles on the left.

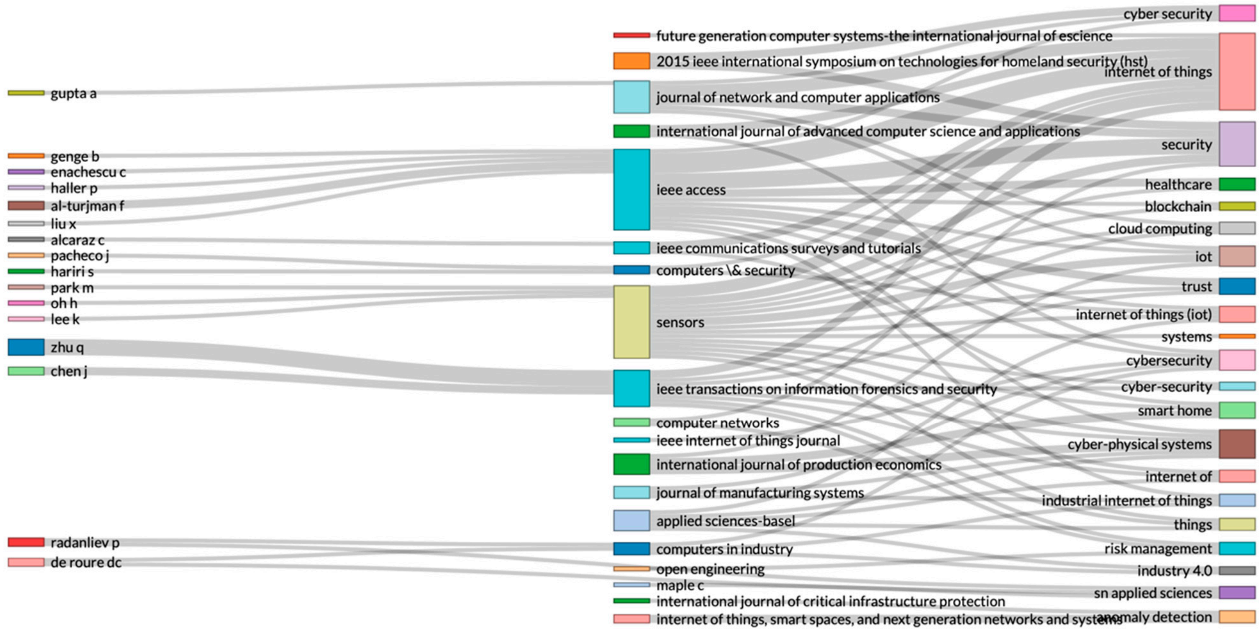

Figure 4. Bibliometric analysis—three-fields plot: keywords from journal sources in the middle, keywords from the articles on the right, and most relevant authors on the left (as determined by the software).

From the bibliometric analysis in Figures 3 and 4, we can see that the topics of IoT, risk, ethics, and healthcare are present in research studies, but the connection between these topics is still in its infancy. To analyse this further, we designed a co-occurrence network (in Figure 5). In the co-occurrence network, we deleted isolated nodes and we tried to visualise how different research topics are related.

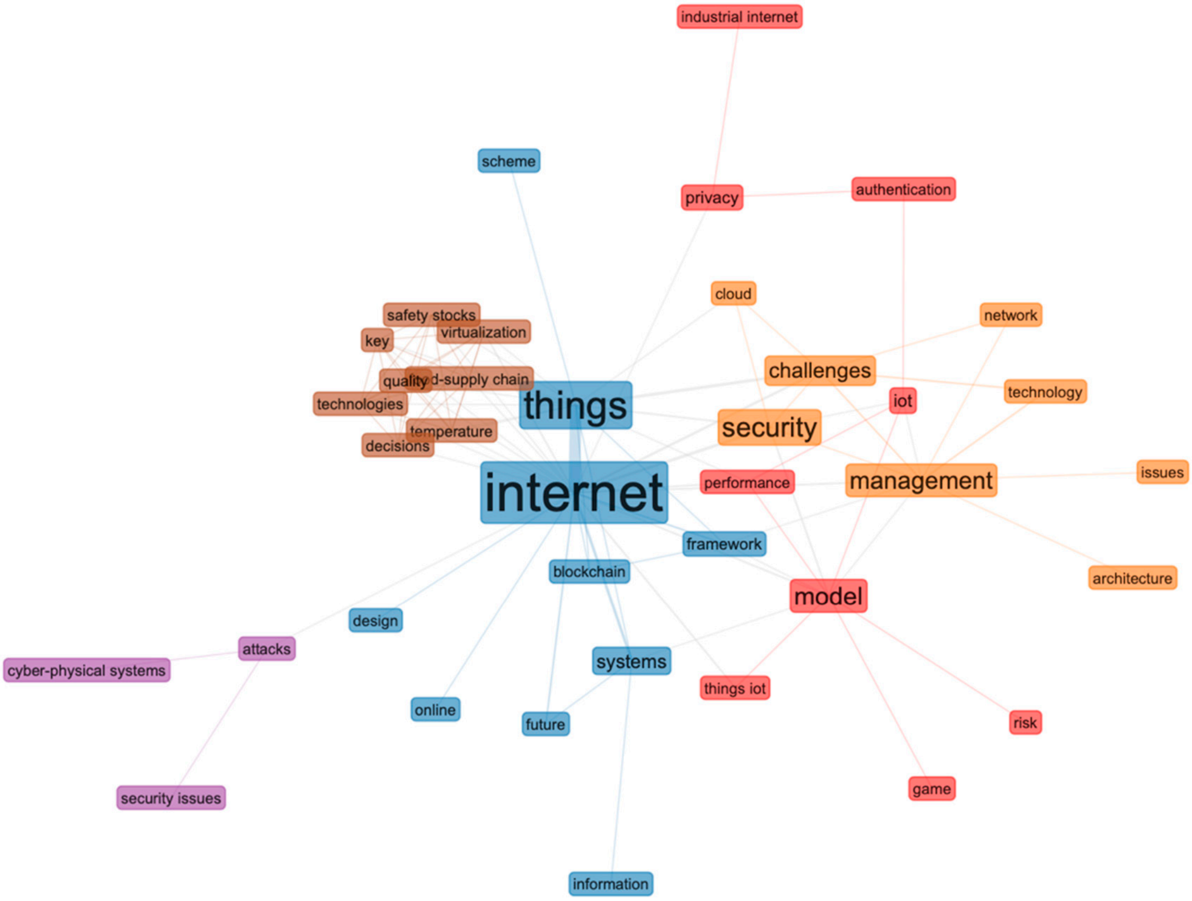

Figure 5. Bibliometric analysis—co-occurrence network.

From the co-occurrence network (in Figure 5), we can see the research topics in colour-coded networks. The healthcare supply chain is in the brown network, security in orange, risk in red, and attacks in purple; trust is missing. This analysis confirms that although trust was present in Figure 4, the topic of trust in this data record was not correlated to the research topics we investigated.

Our final data file to search for correlations between ethics, shared responsibility, health policy, and IoT contained 20 records from a separate search on 'ethics, AND cyber risk'. From this limited data record, when analysed with the R 'bibliometrix' package (Figure 6), we extracted some interesting findings. What this data record shows is that research on these topics is strongly represented by the USA, the UK, and Australia, and is predominantly related to military in the USA and to war in the UK (see Figure 6). There are almost no records of shared responsibility and health policy. We cannot argue that these findings from a limited data record represent all research that exists. However, it is worth mentioning that the search for data records we conducted was from the Web of Science Core Collection and it included all historical records from 1900 to 2020 on the topics of 'ethics, AND cyber risk'. We detail our search parameters in the spirit of reproducible research and we include our data records used in plotting Figure 6 for other researchers to re-analyse.

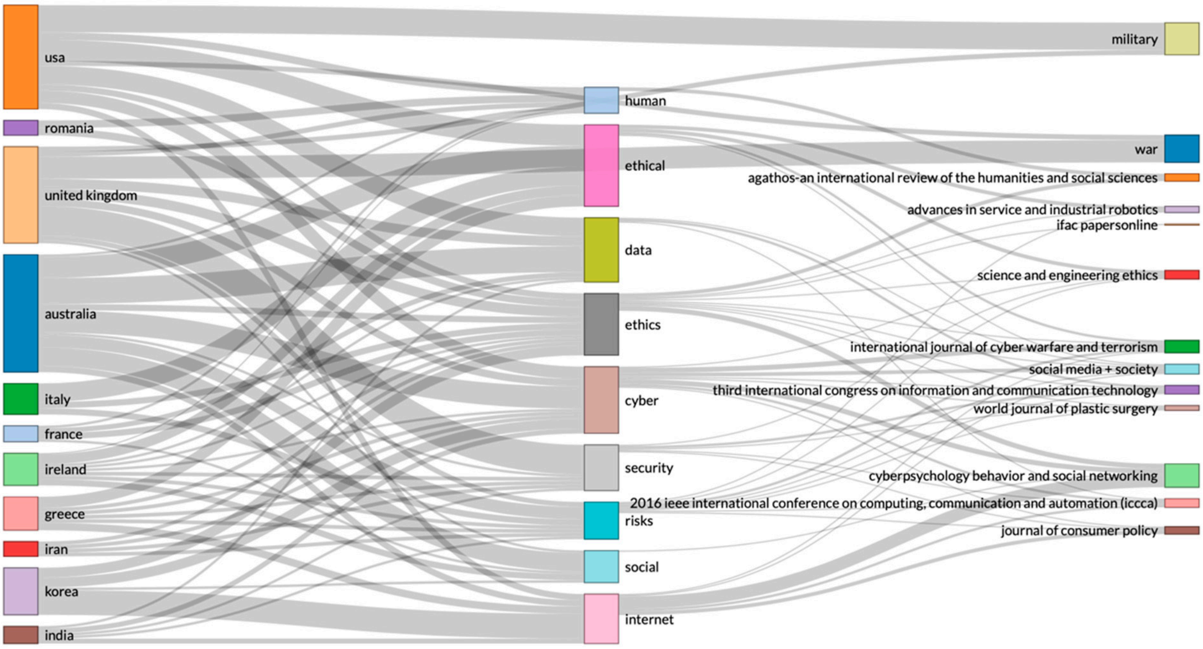

Figure 6. Bibliometric analysis—three-fields plot from the data record on 'ethics, AND cyber risk', relating research papers by country on the left, by source on the right, and by common words association from the records' abstracts in the middle field.

If the research parameters are changed to 'ethics, OR cyber risk', this figure changes significantly, but that would represent a bibliographic analysis of records that include either of the two topics and would not represent scientific records that are related to both topics. To describe the difference between this simple difference in search between 'AND'/'OR', we conducted a search on the Web of Science Core Collection and changed parameters to 'ethics, OR cyber risk'. The search resulted in 155,931 records (in Figure 7), which is significantly more than the 20 records on 'ethics, AND cyber risk' used to plot the Figure 6. To produce the same three-fields plot with this data record, we could use the R studio. R is designed for analysing big data and can handle such large data records. The Web of Science Core Collection, however, only allows extracting 500 records at a time. To create a data file of these records, we would need to extract 311 separate files, and then merge these files before we could upload the data record in the R 'bibliometrix' package. If this data record was considered relevant to ethics, shared responsibility, health policy, and IoT, we could have engaged in such labour intense data collection, but such data record would have simply presented a graph of research on either of the two topics, not research relating the two topics. To analyse the 155,931 records, we used the Web of Science record analysing tool.

To identify if the research on 'ethics, OR cyber risk' is related to shared responsibility and health policy of IoT systems, or also predominated by the research sources on 'military' and 'war' as identified in the Figure 6, we also categorised the 155,931 records in research areas (in Figure 8) and institutions (in Figure 9).

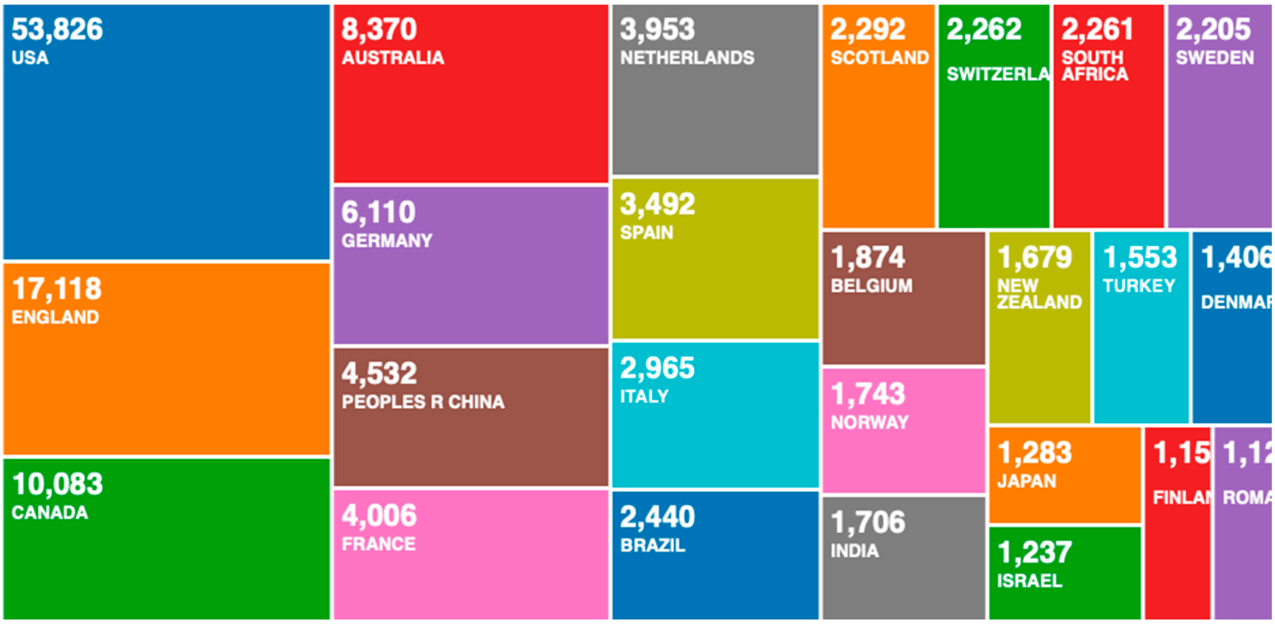

Figure 7. Country categorisation of 155,931 records on 'ethics, OR cyber risk', analysed with the Web of Science record analysing tool.

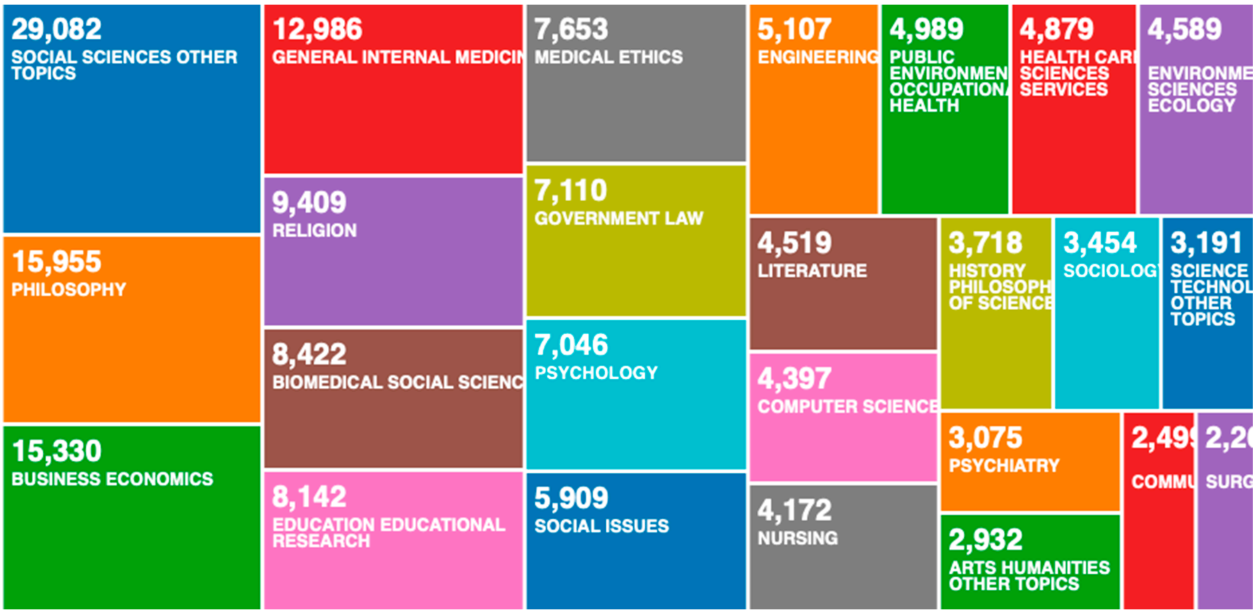

Figure 8. Research areas categorisation of 155,931 records on 'ethics, OR cyber risk', analysed with the Web of Science record analysing tool.

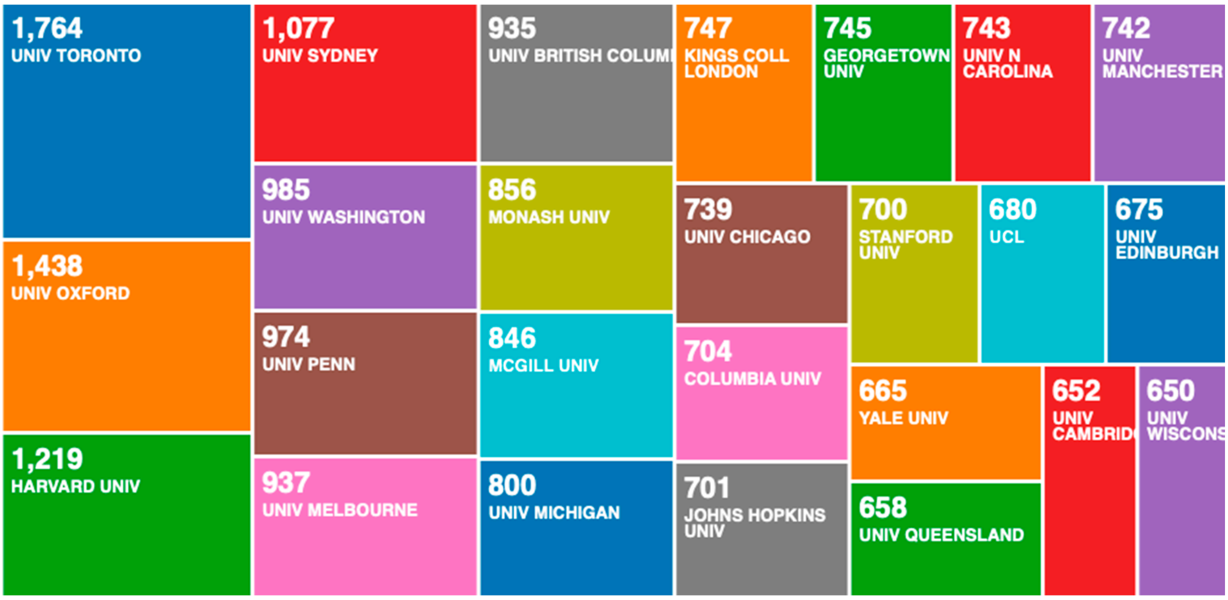

Figure 9. Research institutions categorisation of 155,931 records on 'ethics, OR cyber risk', analysed with the Web of Science record analysing tool.

What the categorisations in Figures 8 and 9 show is that scientific research on 'ethics, OR cyber risk' is strongly present in the research areas on social sciences, but there are also a significant number of records on medical ethics and healthcare sciences. The categorisations in Figures 8 and 9 also show that scientific research on 'ethics, OR cyber risk' is predominately undertaken by academic and not military institutions. Some of these academic institutions also lead the research in ethics, shared responsibility, health policy, and IoT.

The reasons why the USA and the UK are strongly represented in Figure 6 can be explained in the categorisation in Figure 7, which confirms the USA and the UK (along with Australia) as the leading countries for research on 'ethics, OR cyber risk'. This, however, does not explain why research on 'ethics, AND cyber risk' is predominated in the research sources of 'military' and 'war' (see Figure 6). It does however justify our argument that such research is needed in other research areas that are not related to 'military' and 'war', for example, ethics and cyber risk from IoT-connected devices in health policy.

2.1. Explanation on the Limitations of Our Data Records

Since we could not find records that included all search keywords on ethics, shared responsibility, health policy, and IoT, we had to separate the search keywords. Even before we applied statistical software to these results, we knew that these research records would not be directly related to shared responsibility and health policy. Instead, we used the data records to visualise the connection between different keywords.

A particularly interesting result emerged when we searched for: 'Internet of Things, OR ethics, OR cyber risk' (analysed in Figures 10 and 11). We found 199,902 records, which confirmed that these subjects are studied excessively in isolation or with other research topics, but there is very little research on how IoT technology created new cyber risks and what the ethical concerns of this new risk in shared responsibility and health policy for IoT systems are.

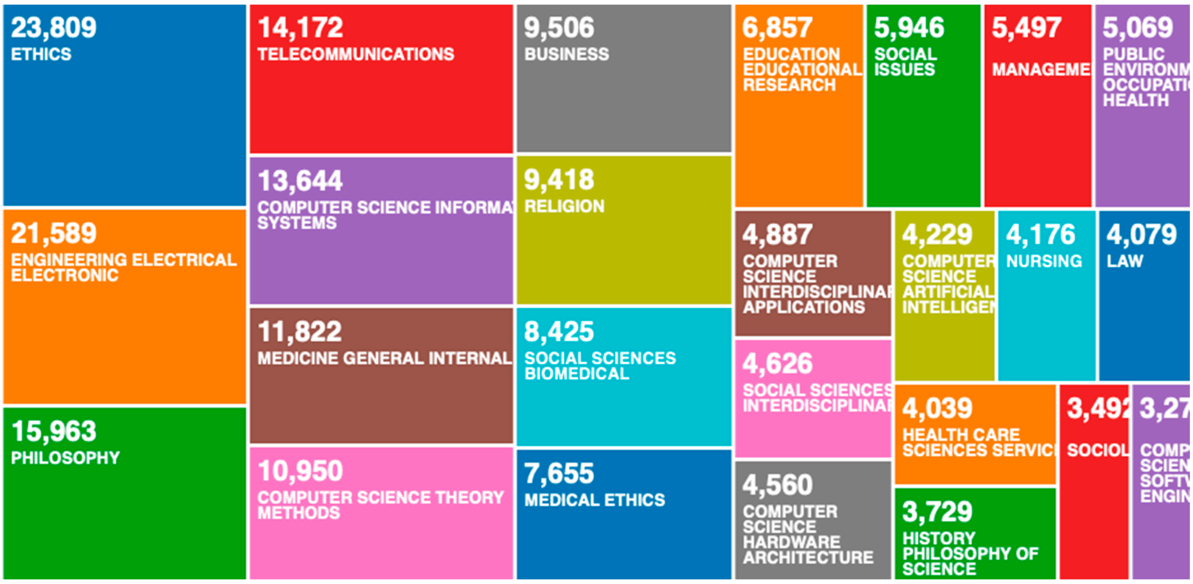

Figure 10. Scientific research from 199,902 records by field—TOPIC: (ethics) OR TOPIC: (cyber risk) OR TOPIC: (internet of things).

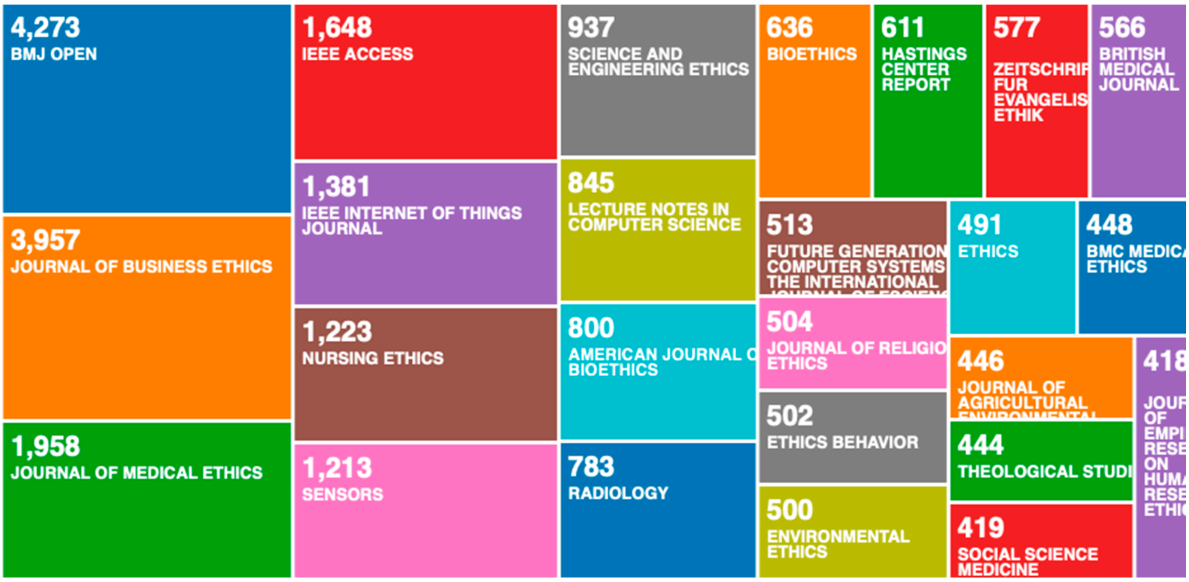

Figure 11. Scientific research from 199,902 records by journal—TOPIC: (ethics) OR TOPIC: (cyber risk) OR TOPIC: (internet of things).

2.2. Summary of the Bibliometric Analysis

In the bibliometric analysis, this paper provides an extensive review of the research on the ethical issues in relation to cyber risk from IoT. Considering that healthcare systems have been studied for much longer than IoT has been in existence, we conducted an extensive review on specific healthcare aspects of IoT in ethics, shared responsibility, and health policy. There are fundamental differences between the bibliometric analysis, which was conducted with statistical methods, and the case study, which was conducted with epistemological analysis. The objective of the case study was to relate a multiverse of keywords on ethics, shared responsibility, health policy, and IoT in an epistemological framework that connects the topics of ethics and shared risk.

The bibliometric analysis showed that there are 'white spots' in scientific research on the topics of IoT and the ethics of shared cyber risk in health policy. This is made clear in our search for data records and analysis on the topics of 'Internet of Things, AND ethics, AND cyber risk'.

Nevertheless, this is not an attempt to persuade the reader that there is no scientific research on these individual topics, as seen in our search results (199,902 records in Figures 10 and 11) for data records on 'Internet of Things, OR ethics, OR cyber risk'.

Our conclusion from the bibliometric analysis is that research on 'Internet of Things, AND ethics, AND cyber risk' is limited, but to say that little research has been conducted on the topic of 'ethics OR cyber risk' (155,931 records in Figure 9) or on shared risks from IoT systems in health policy could be misleading. Such research does exist, as described in (Figures 10 and 11). However, the statistical analysis we conducted shows that such research does not connect the topics of shared responsibility and health policy with the research on IoT, ethics, and cyber risk.

Finally, in the bibliometric analysis, we focused primarily on the topics of ethical research on IoT and cyber risk, and we conducted a separate case study on shared responsibility and health policy when COVID-19 was in its infancy. Hence, we distinguished in our analysis between ethics, shared responsibility, health policy, and IoT prior to the emergence of COVID-19. Although COVID-19 emerged in late 2019, the research on COVID-19 started emerging in 2020 and the adoption of IoT technologies in health policy has taken much longer. We argue that since some of the most prominent literature on ethics, shared responsibility, health policy, and IoT are from prior to COVID-19 emergence, the use of modern technologies was not considered as strongly in the development of those studies. Therefore, the case study was used to extract knowledge from established technological approaches to change that were designed prior to the emergence of COVID-19, the integration of IoT in healthcare, and its associated cyber risk. We then used an epistemological approach to use that knowledge in our study.

3. Case Study as Research Methodology in Combination with Epistemology

An epistemological framework in this paper is defined as a process that derives insights from existing knowledge and represents a method for providing guidance for applying knowledge in practice.

The epistemological approach is used here as a method that provides clarity in blurred subjects. The reason ethical risks in IoT-enabled health policy are considered a 'blurred subject' in this study is the bibliographical analysis in the previous section. Shared responsibility represents a healthcare system where all participants are working towards a common goal, but in COVID-19 management systems, individual healthcare participants are interested in managing COVID-19 and no other illnesses. Healthcare system do not share profits, but are designed to lower cost and deliver service, among many other functions; each participant in the healthcare system is responsible for managing their own department, hence, the primary concern is with eliminating that specific medical problem. However, for the system to operate, participants should be concerned about shared responsibilities. This raises questions on who is responsible for investing in the cybersecurity of medical devices. Is cybersecurity on shared IoT technology an investment in healthcare or an expenditure? If intelligence data are collected from patients, who owns those data? Who is responsible for compliance with regulations? Such blurred subjects are frequently researched with more flexible qualitative methods [4,5], such as case study research.

The research methodology adopted for our article's research is qualitative and explorative in nature, using primary and secondary data resources. The data are synthesised using case study research methodology, using qualitative primary and secondary resources, and categorising emergent ethical concepts into themes.

Academic literature is consulted extensively, then a case study research methodology is applied to build an epistemological framework from the literature review [6]. The case study method is applied with the ethnographic and discourse approaches [7], for the construction of scientific theory [8] on the ethics of shared cyber risks.

The methodology we selected for ensuring validity of the findings is focused on applying qualitative research techniques that include open and categorical coding to analyse and categorise the qualitative data [9–11]. The qualitative data are collected from journals on the topics of shared risk from IoT technologies and cyber risk in the IoT. Open coding was used to validate that there is a reliable representation of the data collected, while categorical coding was subsequently applied to recognise the profounder concepts in the data [12]. Discourse analysis was applied to evaluate and interpret the connotation behind the explicitly stated approaches [11], along with tables of evidence [13] and conceptual diagrams [14] to present graphical analysis.

3.1. Case Study

The case study began by requesting that participants define an overall health, care, and health technology objective as an ethical approach for applying IoT technology to manage COVID-19. Given the difficulties in conducting in-person case study interviews and workshops during COVID-19 lockdowns, the case study was performed with a limited number of the most crucial participants, and these limitations with participants size were enhanced with bibliometric and statistical analysis of data records from the Web of Science databases. To overcome the limitations, a literature review was also performed on this topic and the results were analysed with the case study method (see summary map in Table 1). The pool of 20 participants interviewed were proportionally representative of different levels of seniority and included Senior Directors, Principal Engineers, and Risk Managers. The statistical data of these interviews were analysed, condensed, anonymised, and presented (see Figures 12–16) with the use of the Pugh controlled convergence method [15]. The initial participants were selected through convenience sampling. We conducted semi-structured interviews and we gained informed consent for the study. Only some of the interviews were predetermined in the initial selection and the remainder were chosen based on the development of the case study research. This process corresponded with existing literature [16]. The length of the interviews was predetermined as one hour, and the data collected were transcribed and categorised with aims to investigate the ethical relationship between the notion of IoT and the associated shared responsibility. Following the advice from recent literature on ethical assessments of COVID-19 healthcare strategies [17], the aim of the analysis was to identify the ethical ideas behind the statements and to relate them, in Figure 12, with the categories of ‘nominal’ or ‘desired’ ethical strategy [17].

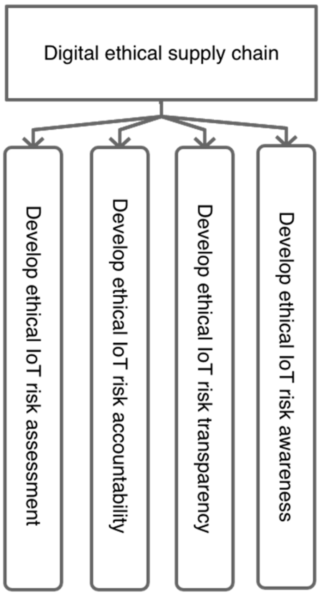
Digital ethical supply chain
Develop ethical IoT risk assessment
Develop ethical IoT risk accountability
Develop ethical IoT risk transparency
Develop ethical IoT risk awareness

Figure 12. Categorising an ethical ‘nominal’ strategy for using IoT technology in health policy for shared responsibility.

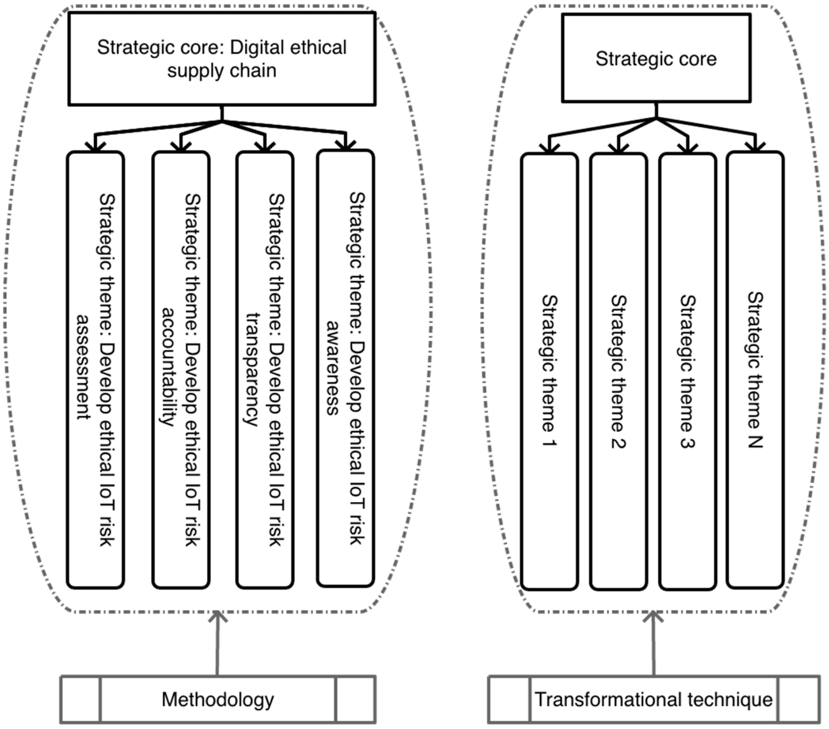
Strategic core: Digital ethical supply chain
Strategic theme: Develop ethical IoT risk assessment
Strategic theme: Develop ethical IoT risk accountability
Strategic theme: Develop ethical IoT risk transparency
Strategic theme: Develop ethical IoT risk awareness
Methodology
Strategic core
Strategic theme 1
Strategic theme 2
Strategic theme 3
Strategic theme N
Transformational technique

Figure 13. Open and categorical coding methodology for applying the epistemological framework in health policy for shared responsibility.

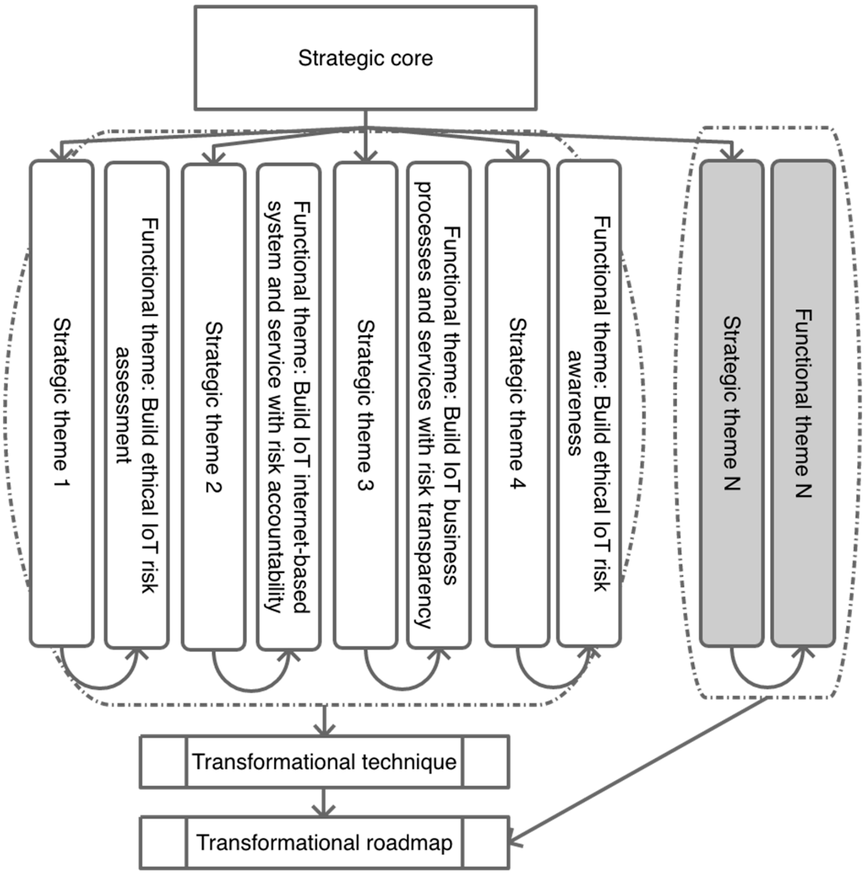
Strategic core
Strategic theme 1
Functional theme: Build ethical IoT risk assessment
Strategic theme 2
Functional theme: Build IoT internet-based system and service with risk accountability
Strategic theme 3
Functional theme: Build IoT business processes and services with risk transparency
Strategic theme 4
Functional theme: Build ethical IoT risk awareness
Strategic theme N
Functional theme N
Transformational technique
Transformational roadmap

Figure 14. Populating the design process for the 'nominal' part of the epistemological framework on awareness, transparency, accountability, and ethical assessment of shared risks in health policy for shared responsibility in IoT systems.

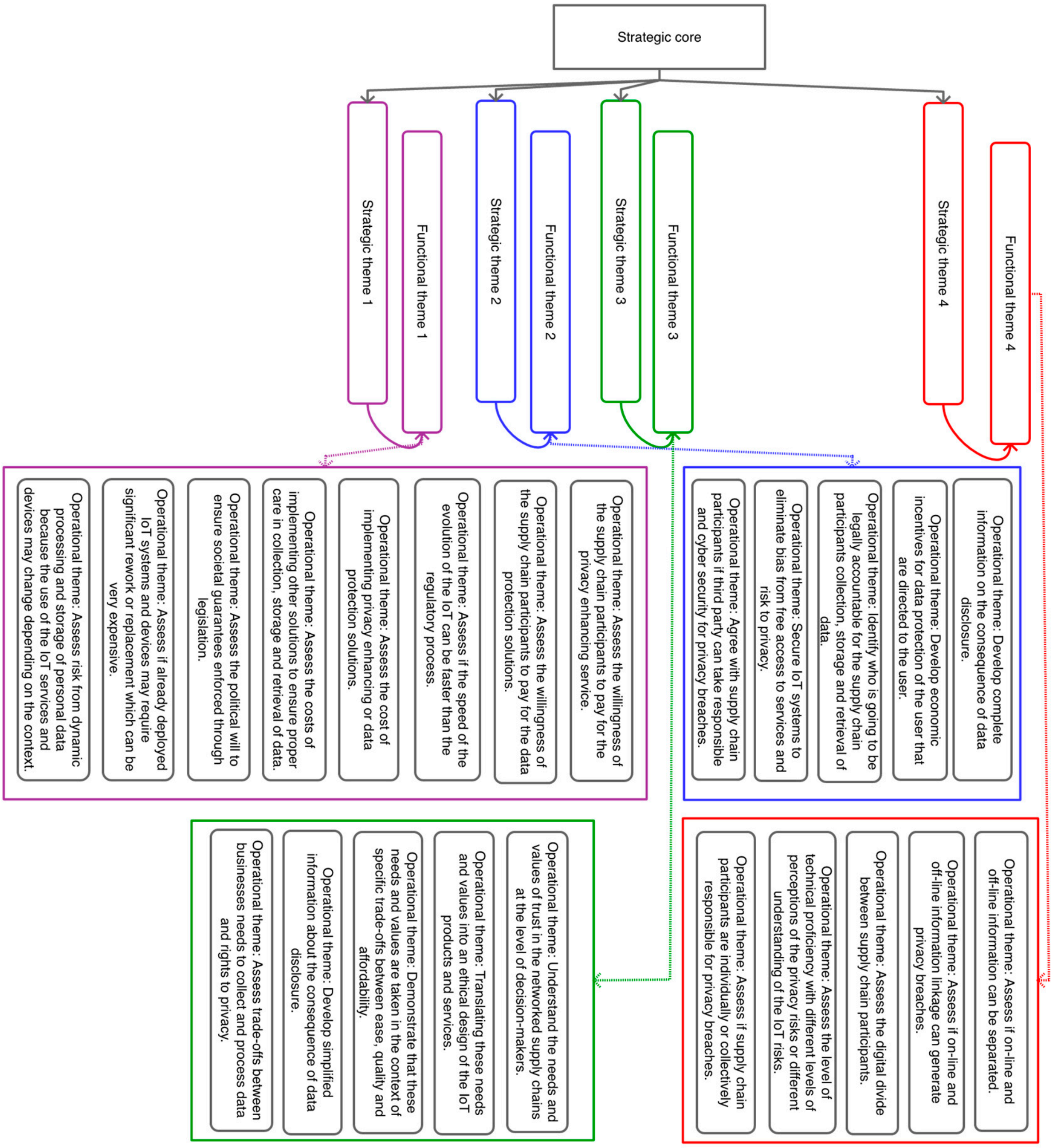
Strategic core
Strategic theme 1
Functional theme 1
Strategic theme 2
Functional theme 2
Strategic theme 3
Functional theme 3
Strategic theme 4
Functional theme 4
Operational theme: Assess the willingness of the supply chain participants to pay for the privacy enhancing service.
Operational theme: Assess the willingness of the supply chain participants to pay for the data protection solutions.
Operational theme: Assess if the speed of the evolution of the IoT can be faster than the regulatory process.
Operational theme: Assess the cost of implementing privacy enhancing or data protection solutions.
Operational theme: Assess the costs of implementing other solutions to ensure proper care in collection, storage and retrieval of data.
Operational theme: Assess the political will to ensure societal guarantees enforced through legislation.
Operational theme: Assess if already deployed IoT systems and devices may require significant rework or replacement which can be very expensive.
Operational theme: Assess risk from dynamic processing and storage of personal data because the use of the IoT services and devices may change depending on the context.
Operational theme: Develop complete information on the consequence of data disclosure.
Operational theme: Develop economic incentives for data protection of the user that are directed to the user.
Operational theme: Identify who is going to be legally accountable for the supply chain participants collection, storage and retrieval of data.
Operational theme: Secure IoT systems to eliminate bias from free access to services and risk to privacy.
Operational theme: Agree with supply chain participants if third party can take responsible and cyber security for privacy breaches.
Operational theme: Understand the needs and values of trust in the networked supply chains at the level of decision-makers.
Operational theme: Translating these needs and values into an ethical design of the IoT products and services.
Operational theme: Demonstrate that these needs and values are taken in the context of specific trade-offs between ease, quality and affordability.
Operational theme: Develop simplified information about the consequence of data disclosure.
Operational theme: Assess trade-offs between businesses needs to collect and process data and rights to privacy.
Operational theme: Assess if on-line and off-line information can be separated.
Operational theme: Assess if on-line and off-line information linkage can generate privacy breaches.
Operational theme: Assess the digital divide between supply chain participants.
Operational theme: Assess the level of technical proficiency with different levels of perceptions of the privacy risks or different understanding of the IoT risks.
Operational theme: Assess if supply chain participants are individually or collectively responsible for privacy breaches.

Figure 15. Populating the design process for the 'executed' part of the epistemological framework on awareness, transparency, accountability, and assessment of shared risks in health policy of IoT systems.

This process of categorising concepts clarified individual levels of the ethical assessment of cyber risk in shared healthcare systems for health policy for shared responsibility. The categorising of the ethical 'nominal' strategy enables clarity in the individual levels of IoT technological integration. To categorise the second level, the case study embodied a process of ideas and concepts conceived as an interrelated, interworking set of objectives that enable the development of a systematic understanding of ethics and the cyber risks in health policy for shared responsibility.

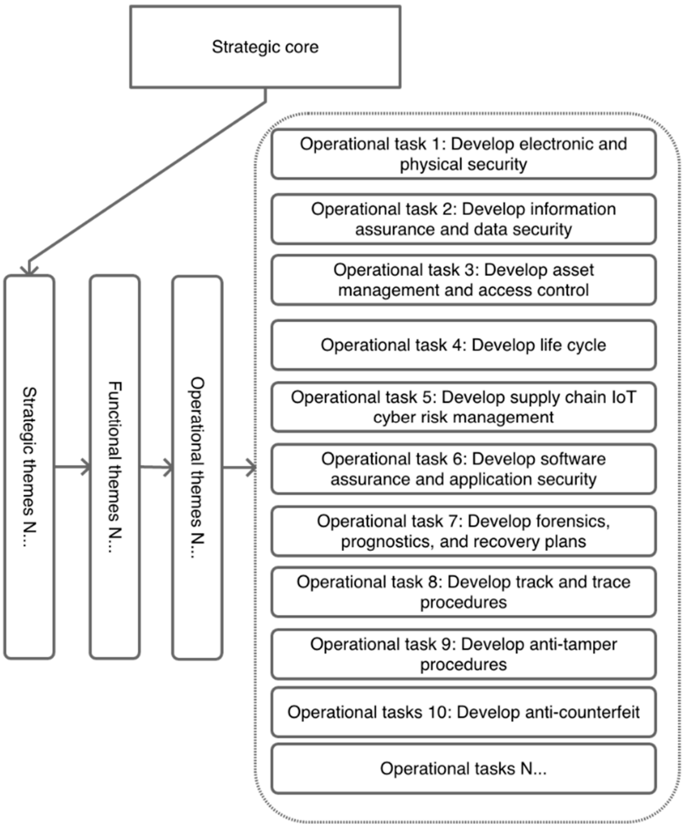
Strategic core
Strategic themes N...
Functional themes N...
Operational themes N...
Operational task 1: Develop electronic and physical security
Operational task 2: Develop information assurance and data security
Operational task 3: Develop asset management and access control
Operational task 4: Develop life cycle
Operational task 5: Develop supply chain IoT cyber risk management
Operational task 6: Develop software assurance and application security
Operational task 7: Develop forensics, prognostics, and recovery plans
Operational task 8: Develop track and trace procedures
Operational task 9: Develop anti-tamper procedures
Operational tasks 10: Develop anti-counterfeit
Operational tasks N...

Figure 16. Populating the final 'operational' step of the epistemological design process for the 'executed' part on awareness, transparency, accountability, and ethical assessment of IoT cyber risk in shared infrastructure for health policy of shared responsibility.

Directive, conventional, and summative analysis were applied to analyse and categorise the ethical concepts emerging from the interviews. Figure 13 outlines sample themes illustrating the stated categories and subcategories relating the concepts with the epistemological framework. The process was built upon the open and categorical coding methodology (Figure 13) to evaluate the epistemological framework.

The diagram in Figure 15 presents a graphical analysis of the framework as a transformational technique that can be applied as a methodology in practice. The graphical analysis represents the step-by-step description of the ethical 'nominal' strategy emerging from the findings from decades of research on ethics, shared responsibility, health policy, and IoT. The process in Figures 12 and 13 enables identifying and relating the functional themes behind individual strategic themes (as described in Figure 12). To verify the design, open coding was applied to provide a 'nominal' representation [18], while categorical coding was applied to identify the profounder concepts [12].

The process describes how open and categorical coding methodology was applied to defining a strategic core, from which the strategic themes emerged as guiding ethical themes. The themes are supported by functional themes, representing ethical action points in the ethical roadmap.

The roadmap as expressed in Figure 14 represents categories of statement. These statements were related to populate the categories of the ethical assessment and continue populating the roadmap (Figure 14) with further ethical themes. The roadmap was designed from the scaffolding in the epistemological framework. The scaffolding utilised the knowledge from the epistemological framework and applied the knowledge for ethical assessment of cyber risk in individual operations from shared healthcare infrastructures. The graphical analysis in Figures 14 and 15 represents the design process for building the complete epistemological framework, required for ethical assessment of the shared cyber risks emerging from IoT technology. To build the complete epistemological framework, we followed the above-described process, and the case study research collected the emerging concepts to categorise and populate the remaining themes.

The graphical analysis in Figure 15 presents the case study design process for building the 'executed' part of the epistemological framework. Detailed summary maps and tables with descriptions of the rationale for each task in Figure 15 and the related references can be found in our project report, which is available as a preprint of earlier work. To avoid duplication of work, we excluded the description tables from this article, but this open-source information would be useful for the readers to better understand the main risks. The design shows the stages of development of IoT technologies and enables awareness, transparency, accountability, and assessment of the cyber risk emerging from individual activities related to the health policy of shared responsibility in IoT systems. The final stage of the epistemological framework is populated in Figure 15 with the operational themes segregated into subcategories of operational tasks. To populate Figure 15, we developed a description table that is presented here as summary map of the literature (Table 1). The summary map in Table 1presents the most critical areas for discovering cyber risks and taking preventative measures against such risks.

Table 1. Summary map of operational tasks.

Operational Themes	References:
Electronic and physical security of real-time data.	[19–21]
Cybersecurity requires information assurance and data security, protection for data in transit from physical and electronic domains and storage facilities.	[22–24]
Asset management and access control are required for granting or denying requests to information and processing services.	[25]
A process is needed to address novel vulnerabilities caused by life cycle issues, diminishing manufacturing sources, and the update of assets.	[26]
IoT cyber risk management requires anti-counterfeit and supply chain risk management to counteract malicious supply-chain components modified from their original design to enable disruption or unauthorised function.	[27,28]
Source code access should be limited to crucial and skilled personnel. This can provide software assurance and application security and may be necessary for eliminating deliberate flaws and vulnerabilities.	[29]
Security should be supported with forensics, prognostics, and recovery plans for the analysis of cyber-attacks and coordination for identifying external cyber-attack vectors.	[26,30,31]
An internal track and trace network process can assist in detecting or preventing the existence of weaknesses in the logistics security controls.	[32,33]
A process for anti-malicious and anti-tamper system engineering is needed to prevent vulnerabilities identified through reverse engineering attacks.	[34]

The operational themes in Figure 15 are linked with emerging operational tasks (in Figure 16). Identically to the process described previously, the case study was used to collect qualitative data and to categorise the propounding concepts in the data.

This design process (Figure 16) for cyber risk provides graphical guidance with themes and subcategorised tasks for the ethical assessment of IoT cyber risk in health policy for the shared responsibility of IoT systems. The epistemological design enables practitioners to assess the strategic, functional, and operational cyber activities and provides a guidance map for ethical cyber assessment.

While the IoT-enabled healthcare adoption requires an ethical reference point, the existing healthcare models lacked clarification on shared cyber risk from IoT technologies. By comparing existing models with case study research with industry participants, the final 'operational' step of the epistemological design in Figure 16 demystifies this. The ethical design clarifies the required digital capabilities and IoT digital technology in the operational levels of the digital healthcare design. The epistemological design for assessing shared risks provides practitioners with a step-by-step guidance on how the ethical assessment can be applied to other medical services.

In Figure 17, the entire epistemological framework for ethical assessment is simplified in one generic diagram. This enables researchers and practitioners to compare the epistemological framework, with their existing process for shared responsibility of IoT systems. The generic design outlines a new approach for the ethical assessment of shared cyber risk. The process described in this paper is specific for shared risks from IoT systems in health policy. However, the design process is also generic and could be applied for other types of shared cyber risks.

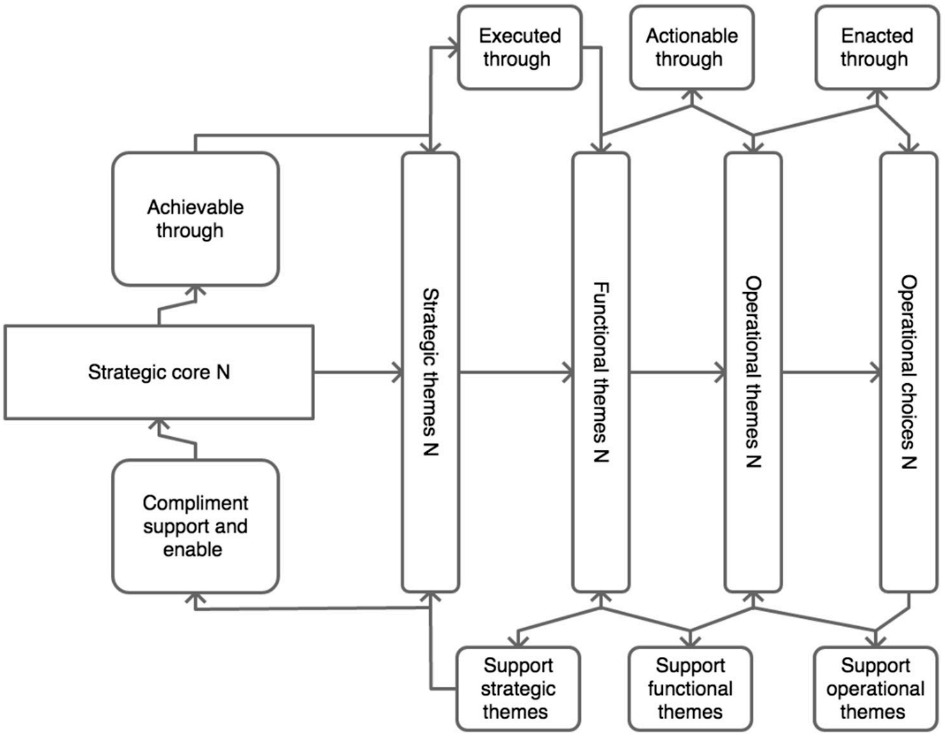

Figure 17. Generic epistemological framework for the ethical assessment of cyber risks from shared infrastructure in IoT systems.

The epistemological framework in Figure 17 pursued common terminology, approaches, and ethical assessment standards while capturing the best practices for shared healthcare elements in medical IoT systems. The findings can be applied as guidance for academics and practitioners for the ethical assessment of shared risks.

3.2. Execution of Tasks

The execution of the tasks is one of the crucial points of relevance for future researchers and practitioners applying the epistemological framework. The key to the execution is in the wording of the strategic, functional, and operational themes and the operational choices. The framework presents a hierarchical structure in the wording, where higher ranked themes present more nominal (descriptive) themes, while the lower ranked themes and choices present imperative statements in the wording. For example, in Figure 12, the example of a 'strategic core' is a statement: 'Digital ethical'. The statement represents an idea as a vision of something to achieve, but it does not detail the process. An example of a 'strategic theme' from Figure 13 would be 'Develop ethical IoT risk awareness'. The wording tells you what to do, but it does not explain how this would be achieved.

An example of a 'functional theme' in Figure 14 is 'Build ethical IoT risk awareness'. The wording tells you how to do the task, but it does not detail the steps. A good example of an 'operational theme' from Figure 15 is the theme 'Develop complete information on the consequences of data disclosure'. The wording explains the steps that need to be completed for achieving the goal of the functional theme, which is in a higher ranking, but falls short of an actionable task that could enable the theme. The final level of the hierarchy is the 'operational choice' or in the second wording 'operational task', where activities are stated as imperative statements. This level represents the operational activity, which is a choice that each company tasks for execution. One example from Figure 16 is the task 'Develop forensics, prognostics, and recovery plans'. The wording of this level is in an imperative form, namely, it tells the organisation what to do in the form of an order. The activity must be clear and executable, otherwise, it would belong to the higher level where themes are more abstract. With this structure of wording, the epistemological framework enables the ethical assessment of cyber risks from shared IoT infrastructure. From the structure of the core, themes, and choices/tasks, all participants would be able to assess the risks of individual strategic, functional, and operational themes, choices, and tasks. This enhances the role of the auditors and the application of due diligence to the health policy of IoT systems.

3.3. Lifecycle of Healthcare Systems and How to Update Task Definitions

In healthcare systems' natural lifecycle, new emerging risks and vulnerabilities are detected and identified continuously. Such risk and vulnerabilities require near real-time process for updating the task definitions. IoT systems present technological advantages for such real-time updates, but without a framework for the risk assessment of medical systems, such updates could become invisible to cybersecurity experts. The framework that we presented enables the visibility of such updates for the ethical assessment of cyber risks from shared IoT infrastructure. For example, when one healthcare department changes the 'Strategic theme', the same department would need to provide detailed descriptions of the tasks/activities that would be performed in the 'Operational choices' further down the hierarchy of the framework. By applying this framework, all the departments in the healthcare system would be able to continuously review any changes in the activities in the digitalisation of medical systems. This resolves a very important issue in healthcare ethics, because currently, individual departments are responsible for performing specific medical functions, but the detailed technological activities of one department are invisible to the remaining departments. The framework we developed resolves this issue and enables all the departments involved to perform the ethical assessment of cyber risks of shared IoT infrastructure and includes the visibility of tasks, definitions, and updates in the entire healthcare systems.

4. Discussion and Main Findings

The epistemological framework enables the ethical assessment to be correlated to the 'themes' and 'categories'. Through the 'themes' and 'categories', the epistemological framework enables the process of identifying ethical conflicts of shared risk in the 'categories', 'activities', and 'operational tasks'. Although the integration of IoT systems can be seen as a strategic decision, associated solely with the participant investing in that IoT system, without identifying the shared cyber risks and the operational and digital capabilities for IoT technologies, it would be impossible to verify if the transfer of cyber risk from one healthcare department to another is ethical. For example, consider the impact on COVID-19 vaccine acceptance if the IoT system is hacked, resulting in a loss of patients' data, and one healthcare department was responsible for installing and maintaining the IoT system that holds shared patients' data. The effect of this cyber-attack will have a negative impact on the entire healthcare system, especially in terms of using new technologies for shared responsibility. There is also secondary loss of cyber risk that needs to be considered and assessed by all the departments that could be affected. It is impossible to understand the potential secondary loss (e.g., impact on vaccine researchers from vaccine producers' brand reputation—e.g., effect on University of Oxford from problems associated with Astra Zeneca, or legal cost of legal proceedings—e.g., EU against Astra Zeneca) without ethical awareness, transparency, and accountability included in the assessment of shared risk and integrated in the medical and healthcare system design. Therefore, the epistemological framework enables the ethical assessment of shared risk, which is crucial for IoT-enabled design.

To design the epistemological framework, we extracted data from the Web of Science Core Collection on the topics of ethics, IoT, and cyber risk. Apart from the Web of Science Core Collection, we also used the Google scholar search engine and other databases of literature to identify studies that relate the topics of ethics, IoT, and cyber risk. We found many studies on different aspects of ethics and IoT, such as the health data of children and IoT or the ethics of cloud computing, even environmental ethics. However, our detailed search on the Web of Science Core Collection failed to identify a single study that relates the topic of ethics, IoT, and cyber risk to the keywords related to ethics, shared responsibility, health policy, and IoT. In our analysis and visualisation of the data records, we also tried searching for related keywords, e.g., searching for 'trust' instead of ethics, or 'privacy' instead of cyber risk. We used statistical methods with R studio to perform bibliometric analysis with the 'bibliometrix' package and to visualise keywords. Our evaluation is explained in the bibliometric analysis section and details our findings that the topic of ethical assessment of shared IoT cyber risks has not been covered extensively.

We followed this conclusion with a case study and applied epistemological reflexivity to the most prominent models on IoT technologies and healthcare systems. We identified a wealth of knowledge on the assessment of shared risk, related to a diverse set of risks, except the ethical assessment of shared risk emerging from IoT systems. This presents a knowledge gap in literature on how digital strategies should be articulated in medical and healthcare systems and how shared risk from connected systems can be assessed in terms of ethics.

5. Conclusions

The findings of this study emerge from the balance between theoretical and technical contributions and are presented in the form of an epistemological framework for the ethical assessment of shared risks in complex and coupled IoT systems. The framework enables ethical awareness, transparency, and accountability in the assessment of new emerging IoT cyber risks in healthcare systems. The epistemological framework emerges from a case study research and bibliometric analysis of existing literature. The epistemological framework in this study utilised and adapted the existing knowledge from keywords emerging from the bibliometric analysis, which included studies conducted prior to the emergence of COVID-19 (and even before the discovery of IoT technologies), and presented a new approach for integrating ethics into the assessment of shared risk in IoT-enabled medical systems. More specifically, the epistemological framework enables ethical awareness, transparency, and accountability in the assessment of shared risks. The epistemological framework is built upon a design that emerges from integrating concepts from models that emerged prior to COVID-19 and IoT, but it incorporates the ethical assessment of shared cyber risks that emerge from IoT technology and COVID-19. This presents a process of shared cyber risks to be assessed through evaluating the IoT operations and differentiates the study from understanding ethics in using IoT technologies in medical systems and the associated cyber risks.

Limitations and Further Research

Finally, the COVID-19 analysis of ethics, shared responsibility, health policy, and IoT in this article stems from a limited number of existing studies on these topics and there is a disparity in the literature on ethics of shared risk from IoT in managing COVID-19, which is still limited. Hence, the balance of comparison on COVID-19 and IoT-enabled medical systems, as subjects in existing literature, lack cohesion. Still, the study applied a bibliometric analysis of large research data records to address the ethical problems in shared risks from IoT systems during the COVID-19 pandemic. The framework in this study represents the first attempt that needs to be further developed by researchers in this field in anticipation of a new Disease X event.

Author Contributions: Conceptualization, P.R. and D.D.R.; methodology, P.R.; software, P.R.; validation, P.R. and D.D.R.; formal analysis, P.R.; investigation, P.R.; resources, D.D.R., data curation, P.R.; writing—original draft preparation, P.R.; writing—review and editing, P.R.; visualization, P.R.; supervision, D.D.R.; project administration, P.R. and D.D.R.; funding acquisition, D.D.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the UK EPSRC [grant number: EP/S035362/1] and by the Cisco Research Centre [grant number CG1525381]. Working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre can be found in pre-prints online.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and this research has been granted ethical approval from the University of Oxford—Medical Sciences: MS IDREC Ethics Committee, under reference R64573/RE001.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data used was obtained from the Web of Science and the detailed process is included in the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Radanliev, P.; De Roure, D.; Walton, R. Data mining and analysis of scientific research data records on Covid-19 mortality, immunity, and vaccine development-In the first wave of the Covid-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 1121–1132. [CrossRef] [PubMed]
2. Aria, M.; Cuccurullo, C. bibliometrix: An R-tool for comprehensive science mapping analysis. *J. Inform.* **2017**, *11*, 959–975. [CrossRef]
3. Jan van Eck, N.; Waltman, L. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics* **2010**, *84*, 523–538. [CrossRef] [PubMed]
4. Nicolescu, R.; Huth, M.; Radanliev, P.; De Roure, D. Mapping the values of IoT. *J. Inf. Technol.* **2018**, *33*, 345–360. [CrossRef]
5. Happa, J.; Nurse, J.R.C.; Goldsmith, M.; Creese, S.; Williams, R. An Ethics Framework for Research into Heterogeneous Systems. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT-2018, London, UK, 28–29 March 2018.
6. Deutsche Forschungsgemeinschaft, R.; Adams, P.; Huggard, P.; Hoare, K. *Forum, Qualitative Social Research*; Deutsche Forschungsgemeinschaft: Bonn, Germany, 2000; Volume 16.
7. Blatter, J.; Haverland, M. *Designing Case Studies*; Palgrave Macmillan UK: London, UK, 2012; ISBN 978-1-349-32085-1.
8. David, M. *Science in Society*; Palgrave Macmillan: New York, NY, USA, 2005.
9. Easterby-Smith, M.; Thorpe, R.; Lowe, A. *Management Research: An Introduction*; SAGE: New York, NY, USA, 2002; ISBN 0761972854.
10. Gummesson, E. *Qualitative Methods in Management Research*; Sage: New York, NY, USA, 2000; ISBN 0761920145.
11. Eriksson, P.; Kovalainen, A. *Qualitative Methods in Business Research*; SAGE: New York, NY, USA, 2008; ISBN 1412903173.
12. Goulding, C. *Grounded Theory: A Practical Guide for Management, Business and Market Researchers*; SAGE: New York, NY, USA, 2002; ISBN 0761966838.
13. Eisenhardt, K.M. Building Theories from Case Study Research. *Acad. Manag. Rev.* **1989**, *14*, 532–550. [CrossRef]
14. Miles, M.B.; Huberman, A.M.; Saldaña, J. *Qualitative Data Analysis: A Methods Sourcebook*; SAGE: New York, NY, USA, 1983; ISBN 1452257876.
15. Pugh, S. *Total Design: Integrated Methods for Successful Product Development*; Addison-Wesley: Boston, MA, USA, 1991; p. 278.
16. Patton, M.Q.; Patton, M.Q. *Qualitative Research and Evaluation Methods*; Sage Publications: New York, NY, USA, 2002; ISBN 0761919716.
17. Radanliev, P.; De Roure, D.; Ani, U.; Carvalho, G. The ethics of shared Covid-19 risks: An epistemological framework for ethical health technology assessment of risk in vaccine supply chain infrastructures. *Health Technol.* **2021**, 1–9. [CrossRef]
18. Charmaz, K. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*; Sage Publications: New York, NY, USA, 2006; ISBN 0761973532.
19. Niggemann, O.; Biswas, G.; Kinnebrew, J.S.; Khorasgani, H.; Volgmann, S.; Bunte, A. Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control. In Proceedings of the International Workshop on the Principles of Diagnosis (DX), Paris, France, 31 August–3 September 2015; pp. 185–192.
20. Almeida, L.; Santos, F.; Oliveira, L. *Structuring Communications for Mobile Cyber-Physical Systems*; Springer International Publishing: Basel, Switzerland, 2016; pp. 51–76.

21. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Comput. Ind.* **2018**, *100*, 212–223. [CrossRef]
22. Rullo, A.; Serra, E.; Lobo, J. *Policy-Based Autonomic Data Governance*; Springer International Publishing: Basel, Switzerland, 2019; Volume 11550, ISBN 978-3-030-17276-3.
23. Bozkus Kahyaoglu, S.; Caliyurt, K. Cyber security assurance process from the internal audit perspective. *Manag. Audit. J.* **2018**, *33*, 360–376. [CrossRef]
24. Toro, C.; Barandiaran, I.; Posada, J. A Perspective on Knowledge Based and Intelligent Systems Implementation in Industrie 4.0. *Procedia Comput. Sci.* **2015**, *60*, 362–370. [CrossRef]
25. Committee on National Security Systems. *National Information Assurance (IA) Glossary*; Fort George G. Meade: Fort Meade, MD, USA, 2010.
26. DiMase, D.; Collier, Z.A.; Heffner, K.; Linkov, I. Systems engineering framework for cyber physical security and resilience. *Environ. Syst. Decis.* **2015**, *35*, 291–300. [CrossRef]
27. Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. *Comput. Ind. Eng.* **2019**, *135*, 582–592. [CrossRef]
28. Soon, J.M.; Manning, L. Developing anti-counterfeiting measures: The role of smart packaging. *Food Res. Int.* **2019**, *123*, 135–143. [CrossRef] [PubMed]
29. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-Physical Systems: The Next Computing Revolution. In Proceedings of the 47th Design Automation Conference-DAC'10, New York, NY, USA, 13–18 June 2010; ACM Press: New York, NY, USA, 2010; p. 731.
30. Zio, E. The future of risk assessment. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 176–190. [CrossRef]
31. Bajramovic, E.; Konys, J.; Zid, I.B.; Lainer, A. Planning the selection and assignment of security forensics countermeasures. *ASME J. Nucl. Eng. Rad. Sci.* **2018**, *4*, 041008. [CrossRef]
32. Stenmanns, J. Logistics from the margins. *Environ. Plan. D Soc. Space* **2019**, *37*, 850–867. [CrossRef]
33. Abdel-Basset, M.; Manogaran, G.; Mohamed, M. Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Futur. Gener. Comput. Syst.* **2018**, *86*, 614–628. [CrossRef]
34. Collier, Z.A.; Hassler, M.L.; Lambert, J.H.; DiMase, D.; Linkov, I. Supply Chains. In *Cyber Resilience of Systems and Networks*; Springer International Publishing: Cham, Switzerland, 2019; pp. 447–462.