electronics

MDPI

Review

A Systematic Mapping Study on Cyber Security Indicator Data

Per Håkon Meland [1,*], Shukun Tokas [2], Gencer Erdogan [2], Karin Bernsmed [1] and Aida Omerovic [3]

[1] SINTEF Digital, Strindvegen 4, NO-7465 Trondheim, Norway; karin.bernsmed@sintef.no
[2] SINTEF Digital, Forskningsveien 1, NO-0314 Oslo, Norway; shukun.tokas@sintef.no (S.T.); gencer.erdogan@sintef.no (G.E.)
[3] Norwegian Computing Center, Gaustadalleen 23a, NO-0373 Oslo, Norway; aida@nr.no
* Correspondence: per.h.meland@sintef.no

Abstract: A security indicator is a sign that shows us what something is like or how a situation is changing and can aid us in making informed estimations on cyber risks. There are many different breeds of security indicators, but, unfortunately, they are not always easy to apply due to a lack of available or credible sources of data. This paper undertakes a systematic mapping study on the academic literature related to cyber security indicator data. We identified 117 primary studies from the past five years as relevant to answer our research questions. They were classified according to a set of categories related to research type, domain, data openness, usage, source, type and content. Our results show a linear growth of publications per year, where most indicators are based on free or internal technical data that are domain independent. While these indicators can give valuable information about the contemporary cyber risk, the increasing usage of unconventional data sources and threat intelligence feeds of more strategic and tactical nature represent a more forward-looking trend. In addition, there is a need to take methods and techniques developed by the research community from the conceptual plane and make them practical enough for real-world application.

Keywords: threat intelligence; data-driven decision making; risk management; data sources; trends

Citation: Meland, P.H.; Tokas, S.; Erdogan, G.; Bernsmed, K.; Omerovic, A. A Systematic Mapping Study on Cyber Security Indicator Data. *Electronics* **2021**, *10*, 1092. https://doi.org/10.3390/electronics10091092

Academic Editors: Changhoon Lee, Yu Chen and Jake Cho

Received: 12 April 2021
Accepted: 30 April 2021
Published: 5 May 2021

1. Introduction

Cyber risk estimates today tend to be based on gut feeling and best guesses. Improved justification and traceability can be achieved through data-driven decisions, but this is not straightforward. With evolving technology and constantly emerging attack methods (and motivations), basing security decisions on past incidents is typically referred to as "driving forward by looking in the rear-view mirror" [1] and cannot be considered reliable. As a remedy to historical data and guesswork, Anderson et al. [2] suggested in 2008 to use forward-looking indicators as an alternative source of decision data, but now, more than a decade later, have we really succeeded in doing this?

The purpose of this paper is to present a systematic mapping study of the literature related to cyber security indicator data. As defined by Kitchenham and Charters [3] and Petersen et al. [4], systematic mapping studies provide an overview of a research area through classification of published literature on the topic. This is somewhat different from systematic literature reviews, which focus more on gathering and synthesizing evidence [4], typically from a smaller set of publications. We identified relevant research and classified their approaches according to a scheme. This contributes to a broad overview of the research field, showing concentrations of effort and revealing areas that need more attention. We then have the possibility to debate if we still base our risk estimates on guts, guesses and past incidents, or whether we have managed to move the field forward, i.e., towards making informed cyber security decisions from relevant indicators. To guide our investigation, we have defined the following research questions:

1. What is the nature of the research using security indicators?
2. What is the intended use of the data?

3. What is the origin of the data for the indicators?
4. What types of the data are being used?
5. What is the data content of the indicators?

The main contributions of this study are: (1) a broad overview of research efforts in the domain of cyber security indicator data; (2) a detailed and reusable classification scheme that can be used to capture new trends in this area using consistent terminology; (3) an analysis of trends within the literature from 2015–2020; and (4) identification of focus areas for further research.

The target audience for this work are researchers and practitioners who want to establish better data-driven practices for cyber risk estimates.

The rest of the paper is structured as follows. Section 2 presents background information about the underlying concepts that are central to our research focus. Section 3 gives an overview of related work and Section 4 presents the methodology used to conduct our systematic mapping study, including search strings, inclusion/exclusion criteria and an overview of the screening process of papers. Section 5 presents the classification scheme that is used to classify primary studies as well as the mapping results. In Section 6, we discuss the result with respect to the research questions, compare our findings with existing research work and recommend possible directions for future work. Finally, Section 7 concludes the paper.

2. Background

The following describes terminology and concepts that are central to our mapping study. An *indicator* is defined by Oxford Advanced Learner's Dictionary [5] as "a sign that shows you what something is like or how a situation is changing". An indicator can for instance be observations of mechanisms and trends within the cybercrime markets, as suggested by Pfleeger and Caputo [6], and indicate relevant cyber threats. One or more *data sources* can be used to determine the status of an indicator. For instance, statistics from a dark net marketplace could be a remote data source, while a system log could be a local data source. There are many possible data sources related to cyber threats, including sharing communities, open source and commercial sources [7]. The term used in the context of sharing such information is usually *threat intelligence*, which is any evidence-based knowledge about threats that can inform decisions [8]. The term can be further defined into the following sub-domains [9,10]:

- *Strategic threat intelligence* is high-level information used by decision-makers, such as financial impact of attacks based on historical data or predictions of what threat agents are up to.
- *Operational threat intelligence* is information about specific impending attacks against the organization.
- *Tactical threat intelligence* is about how threat actors are conducting attacks, for instance attacker tooling and methodology.
- *Technical threat intelligence* (TTI) is more detailed information about attacker tools and methods, such as low-level indicators that are normally consumed through technical resources (e.g., intrusion detection systems (IDS) and malware detection software).

To compare or possibly join data source contents, *metrics* can be useful. Mateski et al. [11] defined a metric to be a standard of measurement and something that allows us to measure attributes and behaviors of interest. An example of a metric is the number of malware sales. A *measure* is a specific observation for a metric, for instance the value 42 for a given week. According to Wang [12], security metrics should be quantitative, objective, employ a formal model, not be boolean (0, 1) and reflect time dependence. There is a plethora of possible security metrics, for instance Herrmann [13] presented more than 900 different ones in her book. The challenge is to find the ones that represent practically useful security indicators.

3. Related Work

We are aware of several review papers, survey papers and mapping studies that partly overlap with ours and provide supplementary material. For instance, Humayun et al. [14] performed a systematic mapping study of common security threats and vulnerabilities from 78 articles, covering studies spanning over a decade (2007–2018). A direct comparison of the study by Humayun et al. [14] and our study is not straightforward, mainly because of the different objectives; for example, Humayun et al. [14] focused on an analysis of publication venue, demography of researchers and key targets of cyber attacks. However, there are common features in the two studies, such as the research methodology, choice of academic databases and domain (i.e., cyber security). They also gave an overview of other mapping studies and systematic literature reviews in the cyber security area. Beyond these, there are many related surveys and reviews that we highlight in the following.

In a publication from 2107, Grajeda et al. [15] analyzed 715 research articles from the years 2010 to 2015 with respect to the utilization of datasets for cybersecurity and cyber forensics. They found 70 different datasets and organized them into 21 categories. The datasets were collected and analyzed from both peer-reviewed articles and Google search (for the datasets that may not have appeared in selected articles). Taking a broader perZheng et al. [16] analyzed their use or creation in nearly 1000 academic papers published between 2012 and 2016. They created a taxonomy for describing the datasets and used machine learning to classify the papers accordingly.spective on datasets for cybersecurity research,

Griffioen et al. [17] evaluated the quality of 17 open source cyber threat intelligence feeds over a period of 14 months and 7 additional feeds over 7 months. Within these, they found that the majority of indicators were active for at least 20 days before they are listed, and that some data were biased towards certain countries. Tundis et al. [18] also surveyed existing open source threat intelligence sources, and, based on interviews with 30 experts (i.e., cyber security professionals and academic researchers), they proposed an approach for the automated assessment of such sources.

In 2016, Pendleton et al. [19] surveyed system security metrics, pointing to big gaps between the existing metrics and desirable metrics. More recently, Cadena et al. [20] carried out a systematic mapping study of metrics and indicators of information security incident management based on 10 primary studies for the period from 2010 to 2019. Our study and that of Cadena et al. [20] share the same motivation, i.e., to support informed security decision-making, but the two differ in addressing terms of research focus. For example, we look into classifying data source, data content, data usage, etc., whereas their focus was on attributes related to cost, quality, service and standards.

In 2018, Husák et al. [21] published a survey of prediction and forecasting methods in cyber security. They also looked at input data for these methods and observed that there are many alternatives with different levels of abstraction. They found that evaluations tend to be based on datasets with high age, which do not necessarily reflect current cyber security threats. Other public datasets are scarcely used or artificially created by the authors to evaluate their own proposed methods. Similarly, Sriavstava et al. [22] found in their review that outdated datasets are used to evaluate machine learning and data mining methods. Sun et al. [23] published in 2019 their survey on datasets related to cyber incident prediction. Nineteen core papers were categorized according to the six data types: *organization's report and dataset*, *network dataset*, *synthetic dataset*, *webpage data*, *social media data* and *mixed- type dataset*.

From their literature survey, Laube and Böhme [24] created a framework for understanding defenders' strategies of privately or publicly sharing cyber security information. They found that, although many theoretical works assume sharing to be beneficial, there is little actual empirical validation.

Diesch and Krcmar [25] investigated the link between information security metrics and security management goals through a literature study. After eliminating duplicates, they found 195 technical security metrics based on 26 articles. They questioned whether all of these are really useful. Kotenko et al. [26] showed how different types of source data

are used in attack modeling and security evaluation. They also provided a comprehensive selection of security metrics.

Gheyas et al. [27] performed a systematic literature review on prediction of insider threats based on 37 articles published between 1950 and 2015. They found that only a small percentage of studies used original real-world data. Tounsi and Rais [9] conducted a survey in 2017 that classified and distinguished existing threat intelligence types and evaluated which were the most popular open source/free threat intelligence tools. They also highlighted some of the problems with technical threat intelligence, such as quality, short-livedness and the overwhelming amount of data, much of it with limited usefulness. Another literature study on threat intelligence by Keim and Mohapatra [28] compared nine of the available open source platforms. They pointed out challenges related to a lack of standardization and ability to select data based on creation date. Samtani et al. [29] reviewed the cyber threat intelligence platforms provided by 91 companies (mostly based in the US). More than 90% of the companies relied either solely or primarily on internal network data. They noted that the Darknet was slowly emerging as a new viable data source for some of the companies. In a literature review on the use of Bayesian Network (BN) models in cyber security, Chockalingam et al. [30] identified the utilized type of data sources. Here, most models used expert knowledge and/or data from the literature, while only a few relied on inputs from vulnerability scanners and incidents data. Furthermore, they found that 13 out of 17 BN models were used for predictive purposes.

4. Methodology

We followed the guidelines and recommendations on systematic mapping studies or scoping studies as proposed by Kitchenham and Charters [3] and Peterson et al. [4,31]. In the planning phase, we established a review protocol, which is an essential element when conducting secondary studies. The review protocol describes the research questions (see Section 1) and methods for conducting the secondary study, such as how the primary studies should be located, appraised and synthesized [32]. Especially when several researchers are involved, a clearly defined protocol reduces the possibility of researcher bias and misconceptions. The following briefly describes the contents of the protocol and implementation.

4.1. Search Keywords

Based on our research questions, we defined an initial set of search keywords, which were used to identify the top relevant papers based on a Google Scholar search. We studied these in detail and applied a *snowballing technique* to find additional papers and a few instances of grey literature that we knew would be relevant. Snowballing refers to using the reference list of a paper, or the citations of the paper, to identify additional papers [33]. The resulting set of 18 core papers were then used as a tool to identify and extract a larger set of keywords. These keywords were then used as basis for defining search strings. As shown in Table 1, we separated between primary keywords to look for in the title and secondary ones for the title, abstract and list of keywords defined by the authors of the primary studies.

Table 1. Primary and secondary keywords.

Title Keywords	Title, Abstract, Author Defined
"cyber security", "information security", "cyber risk", "cyber threat", "threat intelligence", "cyber attack"	"predict", "strategic", "tactical", "likelihood", "probability", "metric", "indicator"

We tested the keywords by checking if they would re-discover the core papers they were derived from. We also removed some superfluous keywords that did not seem to increase the result set. A general observation from experimenting with search strings was

that combinations with only the keyword "security" in the title would be too ambiguous, returning irrelevant results related to the protection of food, animals, borders and climate. Hence, we developed search strings that would either contain keywords "cyber security" or "information security" to improve accuracy of search results.

4.2. Inclusion Criteria

To limit the result set and support the screening process, we defined a set of inclusion criteria, stating that the studies must be:

- related to actual use of indicator data for cyber security risks;
- published between 2015 and 2020 (the selection does not include studies indexed after September 2020);
- written in English; and
- peer-reviewed.

Similarly, our exclusion criteria stated that the studies should not be:

- in the form of patents, general web pages, presentations, books, thesis, tutorials, reports or white papers;
- purely theoretical in nature and with no use of data;
- about visual indicators for tools (e.g., browser extensions);
- addressing topics related to failures, accidents, mistakes or similar;
- repeated studies found in different search engines; or
- inaccessible papers (not retrievable).

4.3. Database Selection and Query Design

In our study, we chose five online databases: IEEE Xplore, Science Direct, ACM Digital Library, SpringerLink and Google Scholar. These were selected because they are central sources for literature related to computer science and cyber security. Google Scholar is not a literature database by itself, but indexes other databases, so there was bound to be some overlap. For each of the databases, we iteratively defined the search string and conducted manual searches within the database, based on the keywords in Table 1. As Brereton et al. [32] observed, the databases are organized around completely different models and have different search functionalities. It was therefore impossible to use the exact same search strings for all five databases, and we had to tailor the search strings individually. The full definitions of the final search strings that we eventually applied can be found in Appendix A. Most databases order results by relevance, and we therefore applied "ten irrelevant papers in a row" as a stopping criterion. In this way, we did not have to go through the complete result set for all search strings.

4.4. Screening and Classification Process

An overview of the search and screening process is given in Figure 1. This process was initiated during September 2020. Researchers A and B independently ran through every search string for all databases and extracted primary studies based on titles. Each of the two result sets where then assessed by the other researcher. The strategy here was that Researcher B voted on papers selected by Researcher A, while Researcher A voted on papers selected by Researcher B. Duplicates were removed and only those studies with votes from both Researchers A and B were selected for the next stage of the screening. This also included papers for which inclusion/exclusion was hard to decide based on title alone. In total, 392 papers were selected at this stage based on title-screening, for the next stage of abstract/summary-based screening. Due to the number of primary studies, four researchers (Researchers A–D) were involved, and we had to calibrate how papers were selected. To do this, 20 papers were randomly picked out for a test screening where all researchers read the abstracts and made a selection. Afterwards, they compared results and discussed deviations to establish a common practice. Following this, the complete set from the title stage were randomized and divided into four groups, one for each researcher. There was no duplication of efforts (double reading) at this stage, and each researcher got a

unique set to screen based on abstract using our inclusion/exclusion criteria. The result set from the abstract stage yielded 219 primary studies.

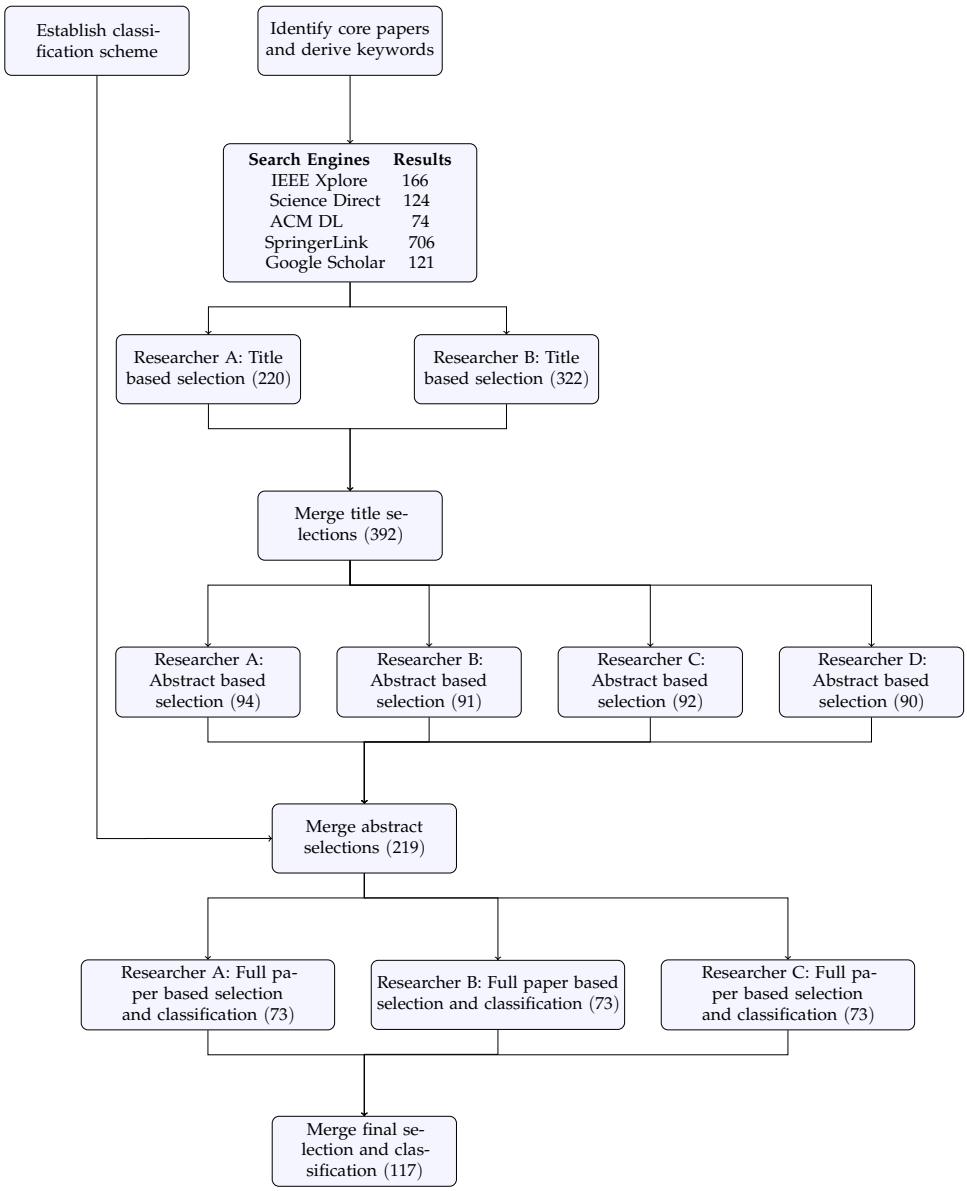

Figure 1. Mapping study flow chart.

Parallel to the screening process thus far, all researchers had been working on developing a classification scheme to address the research questions. It consisted of 46 parameters, which were partly adopted from related work and partly based on what we had observed in the core papers and selected abstracts. To test the classification scheme itself and to calibrate the researchers for classification, we randomly selected 20 primary studies that Researchers A–C read in full and classified accordingly. As before, the researchers compared and discussed their efforts in a joint session.

In the final stage, the complete set of primary studies from the abstract stage were randomized into three unique groups, fully read, classified and merged. This final result set included 117 primary studies, from which the results in Section 5 were derived. The complete list of the selected primary studies is provided in Appendix B.

5. Results

As mentioned in Section 1, systematic mapping studies provide an overview of a research area through classification of published literature on the topic. Thus, in the following, we first present the classification scheme used to categorize the primary studies, and then we present the mapping results with respect to the classification scheme.

5.1. Classification Scheme

The Cyber Security Indicator Data (CSID) classification scheme is illustrated in Figure 2. It covers seven main categories: research type, data openness, data usage, domain, data source, data type and data content. In the following, we describe each category as well as their sub-categories.

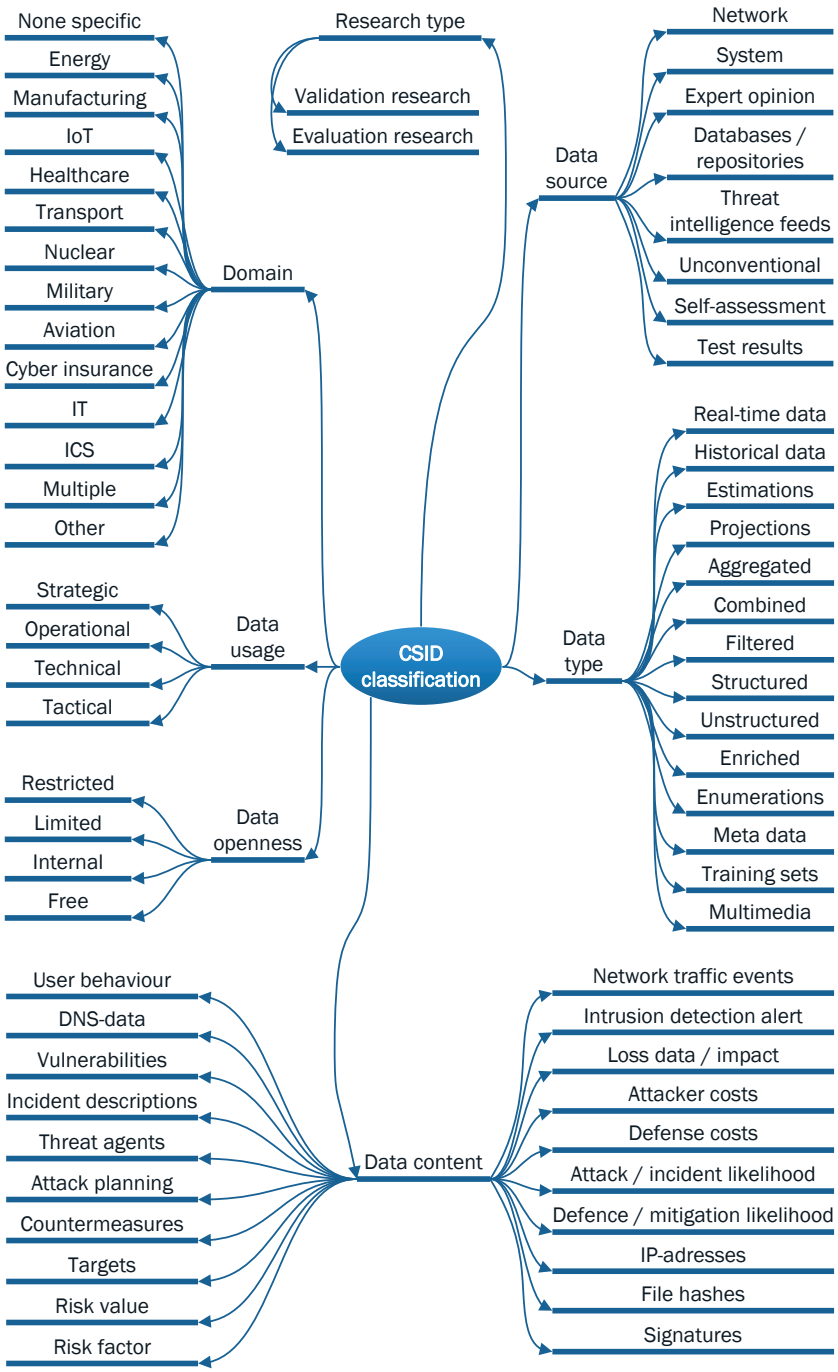

Figure 2. The Cyber Security Indicator Data (CSID) classification scheme.

Research type represents different research approaches. Each primary study included in our systematic mapping study is associated with one research approach. As Petersen et al. did in their mapping study [31], we chose to use an existing classification of research approaches by Wieringa et al. [34]. However, based on the exclusion criteria, we disregarded *solution proposal*, *philosophical*, *opinion* and *personal experience* papers and focused on mapping *validation research*, which describes novel techniques with example experiment/lab data, and *evaluation research*, showing how techniques are used in practice with real data and an evaluation.

Data openness represents the availability of data reported in the primary studies. We distinguish between the following categories of data openness: *free* in the sense that the data are completely open and freely available; *limited* availability where a membership is required to access data; *restricted* access where data are made available to, e.g., authorities; and *internal* access meaning that the data are only accessible from own system(s). We also considered a fifth category, *commercial*, where access to data requires payment. However, none of the primary studies reported on commercially accessible data and this category is therefore disregarded.

Data usage refers to the intended use of data. We consider four categories of data usage: *strategic*, *operational*, *tactical* and *technical*. These categories correspond to the four sub-domains of threat intelligence described in Section 2. Each primary study was associated with one data usage category.

Domain refers to an application domain, including *energy*, *manufacturing*, *IoT*, *healthcare*, *transport*, *nuclear*, *military*, *aviation*, *cyber insurance*, *IT* and *industrial control systems*. In addition, we included three categories to group the primary studies not addressing a specific domain (*none specific*), a combination of different domains (*multiple*) and finally *other* domains.

Data source indicates where the data used in the primary studies originate from. We consider eight non-exclusive data source categories in our classification scheme. *Network* data come from network resources such as firewalls, routers, gateways and DNS-logs. *System* data come from computer resources, typically from internal systems in an organization. *Expert opinion* are indicative variables such as consensus, experience and self-proclamation. *Databases/repositories* provide general data obtained via, e.g., queries. *Threat intelligence feeds* are obtained through subscription-based push services. *Unconventional* data are open source indicators that are either not directly related to the target or not made to predict threats, such as data from marketplaces, forums, blogs and social media. *Self-assessment* data are obtained from internal forms or surveys. *Test results* come from internal tests, typically obtained from tools for penetration testing, vulnerability scanners, etc.

Data type refers to the nature of the data. We consider 14 non-exclusive categories of data type. *Real-time data* are obtained from real-time events via, e.g., sensors. *Historical data* can be log data and recorded frequencies of particular events. *Estimations* are based on incomplete data. *Projections* are made to reflect future values. *Aggregated* data are based on similar content, e.g., aggregated cost. *Combined* data emerge when different data types are used to create other data. *Filtered* data are obtained when values have been removed or masked for some reason, e.g., to preserve anonymity. *Structured* data are clearly defined data types whose pattern makes them easily searchable and interpretable. *Unstructured* data are more difficult to find and interpret, such as audio, video and social media postings. *Enriched* data are improved in some way, e.g., by adding missing details. *Enumerations* are catalogues of publicly known information, such as the Common Weakness Enumeration (CWE) [35]. *Meta data* are data about data, include ontologies and language specification. *Training sets* cover artificial data used for testing, training or simulation. *Multimedia* are mostly temporal media such as video and audio.

Data content refers to the metrics provided by the data sources. We consider 20 non-exclusive categories of data content. *Network traffic events* are recorded events in the network layer that can indicate an attack. An *intrusion detection alert* originates from either network or computer resources. *Loss data/impact* are about the measured effects/costs

of an attack. *Attacker costs* reflect the required investments to successfully perform an attack. *Defence costs* reflect the required investments to successfully mitigate an attack. *Attack/incident likelihood* is a measurement of the (qualitative or quantitative) likelihood of a successful attack or incident. *Defence/mitigation likelihood* is the (qualitative or quantitative) likelihood of a successful defence or mitigation of an attack. *IP-addresses* include blacklisted ones or those with suspicious activity. *File hashes* are used to identify malicious files, such as malware. *Signatures* are code signatures that may be used to identify, e.g., a virus. *User behavior* reflects content about how people interact in a system, e.g., by monitoring the behavior of employees. *DNS-data* can for instance be poisoned DNS servers or addresses. *Vulnerabilities* are descriptions of such found in software/hardware. *Incident descriptions* reflect real security incidents and breaches. *Threat agents* are descriptions of attributing threat agents. *Attack planning* is information obtained from discussions in forums and social media. *Countermeasures* describe recommended preventive or reactive countermeasures for certain threats. *Targets* are descriptions of identified targets exposed to attacks. *Risk value* means the combined likelihood and impact values, i.e., for a specific domain, organization type or size. *Risk factor* contains values related to risks, such as probability, likelihood, frequency, uncertainty, confidence, consequence or impact.

5.2. Mapping Results

In the following, we present the result of our systematic mapping study with respect to the classification scheme described in Section 5.1. A CSV dataset, which includes this scheme and the details of our current classification of primary studies, is available as open research data [36] in order to provide openness, traceability and possible extensions of our work.

As shown in Figure 3, there has been a linear growth in the number of primary studies per year in the period 2015–2020. From being a relatively narrow field with only a handful publications, the increase shows that research on security indicator data is becoming popular. We do not have an exact number for 2020 since the study was conducted before the end of that year. However, the dotted regression line has an annual slope of 7.2, which yields about 40 new publications for 2020.

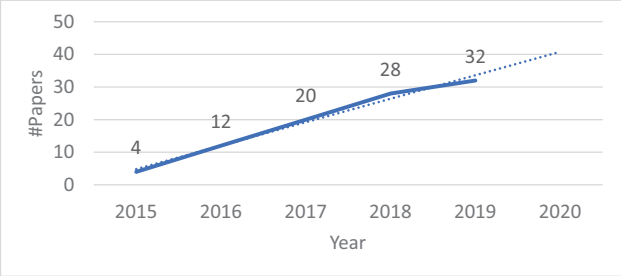

Figure 3. Number of papers per year.

Figure 4 shows a bubble chart illustrating a matrix comprised of the four *data usage* categories (strategic, operational, tactical and technical) and the 14 *domain* categories (energy, manufacturing, IoT, etc., including none specific, multiple and other). Each of the 117 primary studies are grouped in the bubble chart based on a pair of categories (x, y), where x represents a category of domain application and y represents a category of data usage. The numbers in the matrix represent the number of primary studies that fall under each pair of categories, which is also reflected by the size of the bubbles.

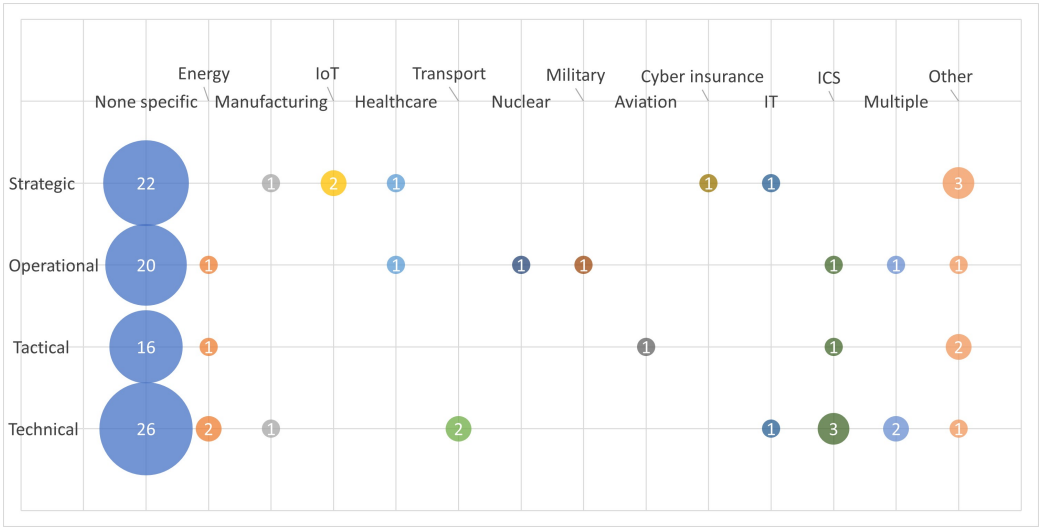

Figure 4. Data usage versus domain.

We can also see from Figure 4 that the majority of the primary studies (84 out of 117) do not address any specific usage domains. Moreover, 26 of these 84 primary studies use technical data, 22 use strategic data, 20 use operational data and 16 use tactical data. Considering the primary studies across all domains from the data usage perspective shows that most of the primary studies use technical data (38), followed by strategic data (31), operational data (27) and tactical data (21). Besides the domain categories *none specific*, *multiple* and *other*, the remaining domain categories are addressed by at least one primary study.

As explained in Section 5.1, we group the primary studies with respect to research type facets. The diagram in Figure 5 shows that the primary studies mostly belong to *validation research* (87 papers), with much less representation within *evaluation research* (30 papers).

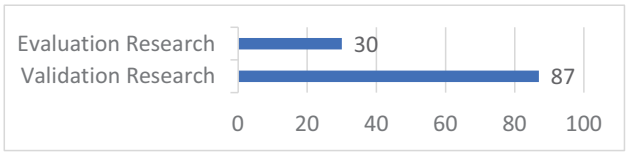

Figure 5. Research type facet.

In terms of data openness, we discovered that the data used in the primary studies mainly fall under the categories *free* or *internal* (see Figure 6). In total, 56 out of 117 (48%) primary studies use data that are *free*, while 46 out of 117 (39%) use *internal* data. From the remaining primary studies, only 12 (10%) use *limited* data and 3 (3%) use *restricted* data. When the study used more than one type of data openness, we classified according to the strictest one.

With respect to the origin of data, we see from Figure 7a that the two most popular data sources are network related data obtained from resources such as firewalls, routers and gateways, as well as system related data obtained from computer resources. Unconventional data, threat intelligence feeds, databases/repositories and expert opinion (see Section 5.1) are other popular resources of data. Note that the data source categories shown in Figure 7a are categories addressed by 20 or more primary studies. The remaining data source categories were addressed by few primary studies (less than 20) and therefore do not represent any significance compared to the counts for the categories shown in Figure 7a. In addition, note that several primary studies include more than one data source.

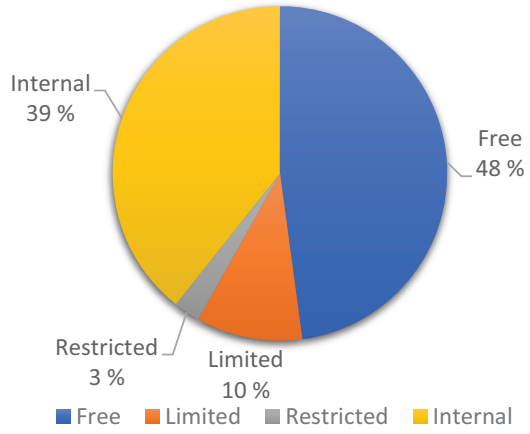

Figure 6. Data openness.

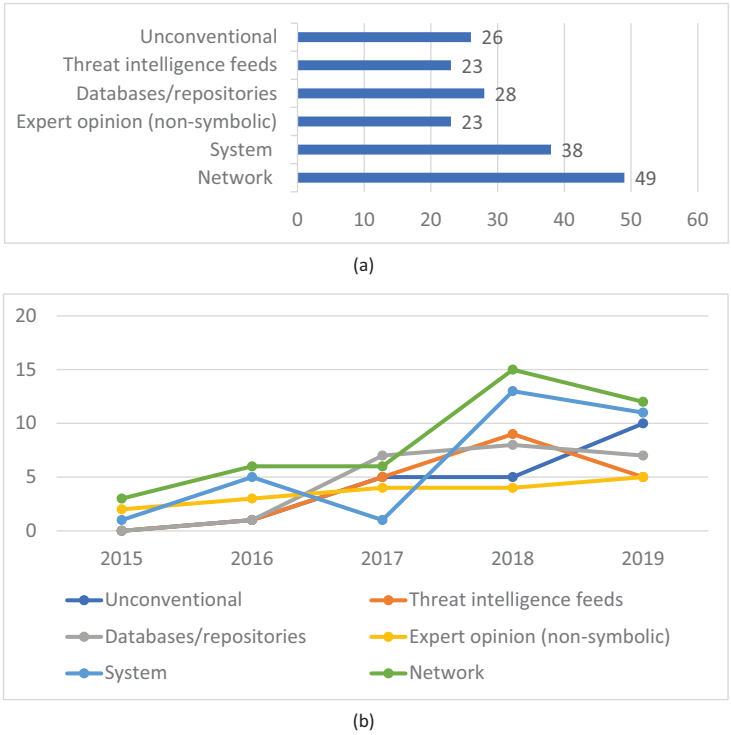

Figure 7. (**a**) Data source categories addressed by 20 or more primary studies; and (**b**) number of primary studies addressing data source categories in the period.

Figure 7b shows the trend for each category over time. We see that the number of papers addressing the categories *system* and *network* have increased the most since 2017, and we also see that the category *unconventional* has increased significantly since 2018.

We applied a similar strategy for presenting the mapping results as described above for the data type and data content categories. Figure 8a illustrates the data type categories addressed by 20 or more primary studies. In this case, we see a pattern of the three most popular groups of data type categories. Figure 8a shows that *structured* and *historical data* are the most popular data type categories, followed by *unstructured*, *combined* and *real-time data* in a shared second place, and finally *training sets* and *estimations* in a shared third place. In terms of the trend for each category over time, Figure 8b shows that *structured* and *historical data* are also the categories that have been increasing the most. Moreover, the categories *unstructured* and *training sets* have increased significantly since 2018.

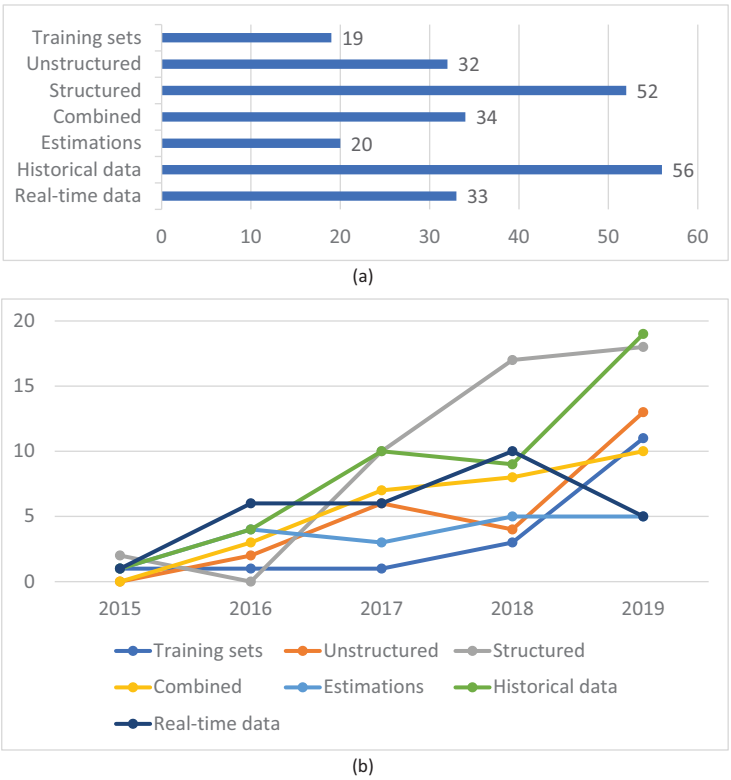

Figure 8. (**a**) Data type categories addressed by 20 or more primary studies; and (**b**) number of primary studies addressing data type categories in the period.

With respect to data content categories, Figure 9a shows that *network traffic event* is the dominating category, followed by *incident descriptions* and *vulnerabilities* in a shared second place, and finally *risk factors* and *IP-addresses* in a shared third place. As for data content categories (cf. Figure 9b), studies on network traffic events have had an increasing trend since 2015, while the remaining categories follow more or less a flat trend since 2015.

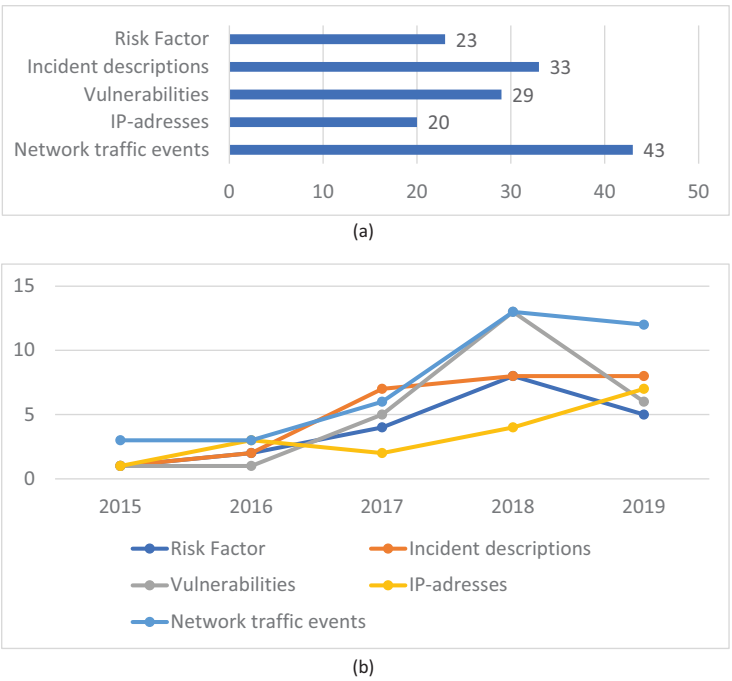

Figure 9. (**a**) Data content categories addressed by 20 or more primary studies; and (**b**) number of primary studies addressing data content categories in the period.

In summary, the observations in Figures 7–9 show that data sources are mainly from network resources such as firewalls, routers and gateways. The data types are mainly structured and historical data, and the data content is mainly related to network traffic events. In terms of trends for data sources, we see an increasing number of papers using system, network and unconventional data sources. Moreover, trends for data types show an increasing number of papers using structured, historical, unstructured and training set data. Finally, trends for data content show that network traffic events is the most increasing category.

Finally, we investigated the average number of data source, data type and data content categories that were considered by the primary studies within the reported period. This average trend will help us understand whether the number of categories used by the primary studies are increasing over time. As illustrated in Figure 10, the usage of data source categories is following a flat trend with the lowest average 1.7 in 2017 and 2019 and the highest average 2.0 in 2018. However, the usage of data type and data content categories are increasing following a linear trend. With respect to data type categories, the lowest average is 1.8 in both 2015 and 2016 and the highest average is 3.0 in 2019. With respect to data content categories, the lowest average is 1.8 in 2016 and the highest average is 3.1 in 2018. Thus, while using multiple data sources has not increased much over the years, the usage of multiple data types and data content is increasing following a linear trend.

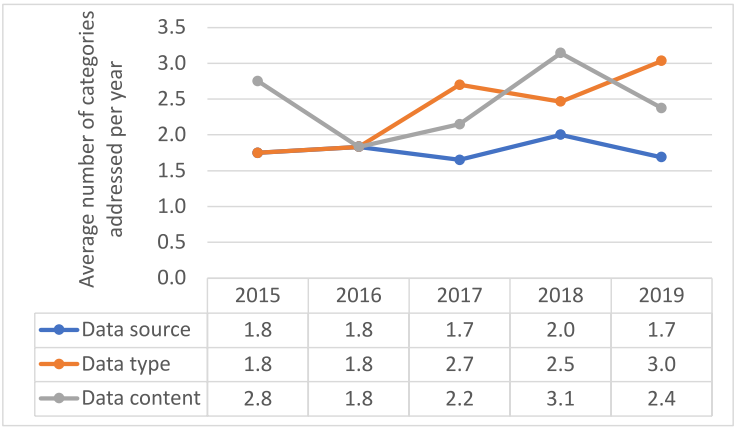

Figure 10. Average number of data source/data type/data content categories per year.

6. Discussion

In this section, we discuss our results with respect to the research questions. We compare our findings with previous work in order to find similarities, address our main limitations and recommend future research.

6.1. RQ 1: What Is the Nature of the Research Using Security Indicators?

As shown in Figure 5, the majority of the papers included in our systematic mapping study were validation research papers (87 out of 117). This is not surprising since, as pointed out by Wieringa et al. [34], the core business of engineering research is to propose new techniques and investigate their properties. However, this implies that most studies lack empirical evaluation with real-world application. It seems to be easier to publish methods and techniques on a conceptual level than to apply them in practice. This is in line with what Pendleton et al. found for security metrics [19], i.e. researchers often encounter a lack of real data for verification and validation.

6.2. RQ 2: What Is the Intended Use of the Data?

The results show that the selected studies are rather evenly distributed in the given data usage categories. In some studies, the data are used for more than one usage category; in such cases, we classified the paper by choosing the broader category. For example, for

technical as well as strategic usage, the study is classified for strategic use as it covers the technical usage. The usage patterns indicate an inclination towards using Technical (38) threat intelligence, which is followed by using Strategic (31), Operational (27) and Tactical (21) data. We consider it positive that the data are used at four levels for informed decision making. However, the studies are sparsely distributed in a wide range of usage domains, with approximately 72% of the selected studies, i.e., 84 of 117, not addressing a specific domain. The sparse distribution of studies within specific domains, mostly 1–2 studies per domain, indicates that research in tapping the potential of threat intelligence at various levels is still in its beginning stages. Chockalingam et al. [30] argued that domain-specific empirical data sources are needed to develop realistic models in cyber security. It can therefore be inferred that more research is needed in domain-specific data usage to contribute to utilizing comprehensive threat intelligence.

6.3. RQ 3: What Is the Origin of the Data for the Indicators?

Our results show that the two most popular data origins were from networks and systems. Unconventional data, threat intelligence feeds, databases/repositories and expert opinion were also quite commonly used (see Figure 7). We consider it positive that real-world data have been increasingly used in the last few years, in particular since the majority of earlier studies are not using real-world data. For example, related to digital forensics, Grajeda et al. [15] showed that the clear majority of datasets are experimentally generated (56.4%), with real-world user generated in second place (36.7%). Furthermore, Gheyas et al. [27] showed that only a small percentage of studies up until 2015 used original real-world data for the prediction of insider threats. Chockalingam et al. [30] also showed in 2017 that most Bayesian Network models used expert knowledge and/or data from the literature as their data sources.

An interesting observation regarding the origin of the data is that each of the primary studies used, on average, more than one data source for deriving their indicators (Figure 10). For example, the approach presented by Erdogan et al. [37] reports four data sources as input for cyber-risk assessment (network layer monitoring indicators, application layer monitoring indicators, security test results and business-related information obtained from stakeholders). While we did not record whether these previous studies have shared the datasets openly with others, the benefits of collecting and sharing such data are pointed out by Moore et al. [38] and Zheng et al. [16].

Close to half (48%) of the input data from the primary studies were free, meaning publicly available. That is somewhat lower than what Zheng et al. [16] registered (76%). This could be explained by the fact that many studies used more than one type of data source, and we classified these according to the strictest type (typically internal).

6.4. RQ 4: What Types of Data Are Being Used?

The trends related to data type indicate that the community is increasingly becoming better in taking advantage of structured and historical data in particular. Wagner et al. [39] showed a precipitously increasing research interest in cyber threat intelligence sharing up until 2016, followed by a slight decline in the following years. One could assume that this is due to improved maturity and uptake of standardized languages for sharing threat intelligence, such as Mitre's STIX [40]. However, studies by Ramsdale et al. [41] and Bromander et al. [42,43] show the contrary and that, in practice, threat intelligence providers are opting for custom or simple formats. We did not classify primary studies according to specific sharing standards or enumerations, and this could be a future extension to the scheme. Mavroeidis and Bromander [44] provided an overview of those already used for sharing threat intelligence. It is also outside of our analysis whether the increasing number of papers are using different data source instances or if they are using the same ones.

The results indicate a recent sharp growth in publications applying unstructured data. We believe this is directly related to the increased usage of unconventional data sources, such as social media. This is in accordance with findings by Husák et al.'s [21] in their

survey of prediction and forecasting methods in cyber security, showing recent approaches based on non-technical data from sentiment analysis on social networks or changes in user behavior.

6.5. RQ 5: What Is the Data Content of the Indicators?

As mentioned in our results, network traffic dominates among the data content types, which conforms with the popular corresponding data source/origin (network) and data usage (technical) classifications. We also found that many of the primary studies did not really give precise information about what kind of network traffic they were using, which is partly the reason we find a high concentration here. For some primary studies, we could classify more precisely towards IP-addresses or DNS-data. In 2016, Pendleton et al. [19] recommended that security publications should explicitly specify their security metrics, but we did not find much evidence of this actually being done. Data about incidents and vulnerabilities also have a technical content, and, as Tounsi and Rais [9] pointed out, these are easy to quantify, share, standardize and determine immediate actions from. Although not directly comparable, Grajeda et al. [15], found utilization of datasets related to malware (signatures), network traffic and chat logs (attack planning and targets), but these were not dominating for forensics. Within the datasets catalogued by Zheng et al. [16], there were content related to vulnerabilities, exploits (incident descriptions), cybercrime activities (attack planning and targets), network traces (network traffic events), user activities (user behavior), alerts (intrusion detection alert) and configurations (countermeasures). Here, the technical content types dominated as well.

6.6. Limitations and Recommendations for Future Research

While a systematic mapping study captures focus areas and trends within the literature, it does not dig into the details and quality of results from the primary studies. Hence, we cannot give any recommendations on which data and indicator types work better than others. That would require a more focused literature review, but it is our impression that the current literature does not contain appropriate and comparable parameters to make such benchmarks.

Due to the empirical nature of systematic mapping studies, threats to validity such as construct validity or internal validity are present. To mitigate threats to validity concerning selection, screening and classification of studies, we defined a detailed screening strategy and screening and classification process. In addition, we carried out a calibration exercise to address variances between researchers. To a considerable degree, the aforementioned measures confirm the validity of the search, screening and classification processes. We also acknowledge that relevant publications may have been overlooked due to missing search keywords, delayed indexing by search engines or human mistakes in the screening process. Despite actions taken to calibrate the participating researchers and reduce systematic errors, the mapping is based on subjective interpretations of paper contents. Due to limited resources, we did not have the opportunity to undertake double review of the complete set of full papers. However, we would argue that we included such a large body of primary studies that the mapping still shows an accurate and precise overall picture.

Our classification scheme is more detailed or has a different focus than what is seen in related work (e.g., Sun et al. [23], Grajeda et al. [15] and Zheng et al. [16]). It is also highly reusable and can be applied to capture new trends by doing a similar study in the future. Furthermore, it would be interesting to include more grey literature (e.g., technical reports, white papers, theses and web pages) to capture use of cyber security indicators that are not driven by academic research. According to Garousi et al. [45], such multivocal literature reviews can be valuable in closing the gap between academic research and practice. This kind of work would require more use of manual search and snowballing, which unfortunately is quite resource demanding.

7. Conclusions

We conducted a systematic mapping study on the use of cyber security indicator data in the academic literature to structure the research area. The number of publications has had a linear growth over the past five years, and the dominant approach is validation research based on free (public) or internally developed indicators. The usage patterns show a slight inclination towards technical threat intelligence, with little use of domain specific data. We can see a trend where data originating from network or system resources are increasing the most, followed by unconventional data, threat intelligence feeds, databases/repositories and expert opinion. On average, more than one data source is used to derive indicators in each paper. Our results show that the research community is eagerly developing new methods and techniques to support security decisions. However, many proposed techniques are on the conceptual level, with little or no empirical evaluation, thus may not yet be mature enough for real-world application. With indicators that are rather technical in nature, we can quickly share information about present security events, increase situational awareness and act accordingly. This allows contemporary cyber risk estimates to become more data-driven and less gut-driven. At the same time, such indicators tend to be short-lived. The increasing usage of unconventional data sources and threat intelligence feeds of more strategic and tactical nature represent a more forward-looking trend. We cannot really say whether or not we have become better at anticipating attacks, but at least it seems the research community is trying.

Author Contributions: Conceptualization, P.H.M., K.B. and A.O.; methodology, P.H.M., G.E. and A.O.; validation, P.H.M., S.T. and G.E.; investigation, P.H.M., S.T., G.E., K.B. and A.E.; resources, P.H.M. and S.T.; data curation, P.H.M., S.T., G.E., K.B. and A.E.; writing—original draft preparation, P.H.M., S.T., G.E., K.B. and A.E.; writing—review and editing, P.H.M., S.T., G.E., K.B. and A.E.; visualization, P.H.M., S.T. and G.E.; supervision, P.H.M.; and project administration, G.E. and A.O. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by CyberSec4Europe, which is funded by the European Union under the H2020 Programme Grant Agreement No. 830929.

Data Availability Statement: The data presented in this study are available at https://doi.org/10.5281/zenodo.4639585.

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

Appendix A. Search String Definitions

For all databases, we tried to create as equivalent searches as possible. However, we had to consider differences in features and functionality. The sections below show how we implemented the queries for each of the databases.

Appendix A.1. IEEE Xplore

The *Command Search* feature of this database allows query strings consisting of data fields and operators (in caps). We also applied a filter to limit the result to publications including and between 2015 and 2020. The following search string was applied:

```
(("Document Title":"cyber security" OR
title:"information security" OR
title:"cyber risk" OR
title:"cyber threat" OR
title:"threat intelligence"
OR title:"cyber attack") AND
("All Metadata":"predict" OR
Search_All:"strategic" OR
Search_All:"tactical" OR
Search_All:"likelihood" OR
Search_All:"probability" OR
Search_All:"metric" OR
```

```
Search_All:"indicator"))
```

Appendix A.2. Science Direct

We made use of the search form instead of a query string for this database. The advanced search feature allowed us to specific keywords for the *title* and another set for the *title*, *abstract* and *author-specified keyword*. However, the space between keywords implicitly meant an AND-operator, while what we really needed was OR. This meant that we had to submit 42 search forms, one for each primary keyword for the title in combination with every secondary keyword for the range 2015–2020.

Appendix A.3. ACM Digital Library

This database allowed searching for specific keywords in title, abstract and author specified keywords. The following search string was applied:

```
[[Publication Title: "cyber security"] OR
[Publication Title: "information security"] OR
[Publication Title: "cyber risk"] OR
[Publication Title: "cyber threat"] OR
[Publication Title: "threat intelligence"] OR
[Publication Title: "cyber attack"]] AND
[[Abstract: predict] OR [Abstract: strategic] OR
[Abstract: tactical] OR [Abstract: likelihood] OR
[Abstract: probability] OR [Abstract: metric] OR
[Abstract: indicator]] AND
[Publication Date: (01/01/2015 TO 12/31/2020)]
```

Appendix A.4. SpingerLink

We employed a form-based (advanced) search. The title search did not allow for operators, hence we had to submit six search forms, one for each primary keyword and where at least one of the secondary keywords appeared somewhere. There was no option to search within just the abstract or author defined keywords, hence the result set became large, and we had to use the stopping criteria (results sorted by relevance, stop after 10 irrelevant in a row). The date range was set to 2015–2020.

Appendix A.5. Google Scholar

The advanced features of this search engine allowed for specifying title keywords, with additional ones using | as an OR operator. It was important to turn off personalized search results (turn off "signed-in search activity") so that different researchers would get the same results. If not, the results would have been influenced by their previous search history. We specifically excluded patents and citations and defined the date range 2015–2020. The following search string was applied:

```
allintitle: ("cyber security" |
"information security"| "cyber risk" |
"cyber threat"| "threat intelligence" |
"cyber attack") (Predict | strategic |
tactical | likelihood | probability |
metric | indicator)
```

Appendix B. The Selected Primary Studies

- Kolosok, Irina and Liudmila Gurina (2014). "Calculation of cyber security index in the problem of power system state estimation based on SCADA and WAMS measurements". In: International Conference on Critical Information Infrastructures Security. Springer, pp. 172–177.
- Liu, Yang et al. (2015). "Predicting cyber security incidents using feature-based characterization of network-level malicious activities". In: Proceedings of the 2015

ACM Inter- national Workshop on International Workshop on Security and Privacy Analytics, pp. 3–9.

- Llansó, Thomas, Anurag Dwivedi and Michael Smeltzer (2015). "An approach for estimating cyber attack level of effort". In: 2015 Annual IEEE Systems Conference (SysCon) Proceedings. IEEE, pp. 14–19.
- Shin, Jinsoo, Hanseong Son, Gyunyoung Heo, et al. (2015). "Development of a cyber security risk model using Bayesian networks". In: Reliability Engineering & System Safety 134, pp. 208–217.
- Zhan, Zhenxin, Maochao Xu and Shouhuai Xu (2015). "Predicting cyber attack rates with extreme values". In: IEEE Transactions on Information Forensics and Security 10.8, pp. 1666–1677.
- Atighetchi, Michael et al. (2016). "Experimentation support for cyber security evaluations". In: Proceedings of the 11th Annual Cyber and Information Security Research Conference, pp. 1–7.
- Aziz, Benjamin, Ali Malik and Jeyong Jung (2016). "Check your blind spot: a new cyber-security metric for measuring incident response readiness". In: International Workshop on Risk Assessment and Risk-driven Testing. Springer, pp. 19– 33.
- Chhetri, Sujit Rokka, Arquimedes Canedo and Mohammad Abdullah Al Faruque (2016). "Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems". In: 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, pp. 1–8.
- Dog, Spike E et al. (2016). "Strategic cyber threat intelligence sharing: A case study of ids logs". In: 2016 25th International Conference on Computer Communication and Networks (ICCCN). IEEE, pp. 1–6.
- Hamid, T et al. (2016). "Cyber security risk evaluation research based on entropy weight method". In: 2016 9th International Conference on Developments in eSystems Engineering (DeSE). IEEE, pp. 98–104.
- Je, Young-Man, Yen-Yoo You and Kwan-Sik Na (2016). "Information security evaluation using multi-attribute threat index". In: Wireless Personal Communications 89.3, pp. 913–925.
- Liao, Xiaojing et al. (2016). "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence". In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 755–766.
- Noble, Jordan and Niall M Adams (2016). "Correlation-based streaming anomaly detection in cyber-security". In: 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW). IEEE Computer Society, pp. 311–318.
- Singh, Umesh Kumar and Chanchala Joshi (2016). "Network security risk level estimation tool for information security measure". In: 2016 IEEE 7th Power India International Conference (PIICON). IEEE, pp. 1–6.
- Wagner, Cynthia et al. (2016). "Misp: The design and implementation of a collaborative threat intelligence sharing platform". In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 49– 56.
- Wang, Jiao et al. (2016). "A method for information security risk assessment based on the dynamic bayesian network". In: 2016 International Conference on Networking and Network Applications (NaNA). IEEE, pp. 279–283.
- Wangen, Gaute and Andrii Shalaginov (2016). "Quantitative risk, statistical methods and the four quadrants for information security". In: International Conference on Risks and Security of Internet and Systems. Springer, pp. 127–143.
- Ahrend, Jan M and Marina Jirotka (2017). "Anticipation in Cyber-Security". In: Handbook of Anticipation. Springer, Cham, pp. 1–28.
- Aksu, M Ugur et al. (2017). "A quantitative CVSS-based cyber security risk assessment methodology for IT systems". In: 2017 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–8.

- AlEroud, Ahmed and Izzat Alsmadi (2017). "Identifying cyber-attacks on software defined networks: An inference- based intrusion detection approach". In: Journal of Network and Computer Applications 80, pp. 152–164.
- Andress, J et al. (2017). "Chapter 10–Information Security Program Metrics". In: Building a Practical Information Security Program, pp. 169–183.
- Bernsmed, Karin et al. (2017). "Visualizing cyber security risks with bow-tie diagrams". In: International Workshop on Graphical Models for Security. Springer, pp. 38–56.
- Best, Daniel M et al. (2017). "Improved cyber threat indicator sharing by scoring privacy risk". In: 2017 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, pp. 1–5.
- Černivec, Aleš et al. (2017). "Employing Graphical Risk Models to Facilitate Cyber-Risk Monitoring-the WISER Approach". In: International Workshop on Graphical Models for Security. Springer, pp. 127–146.
- Cheng, Ran, Yueming Lu and Jiefu Gan (2017). "Environment-Related Information Security Evaluation for Intrusion Detection Systems". In: International Conference on Communicatins and Networking in China. Springer, pp. 373–382.
- Dalton, Adam et al. (2017). "Improving cyber-attack predictions through information foraging". In: 2017 IEEE International Conference on Big Data (Big Data). IEEE, pp. 4642–4647.
- Doynikova, Elena and Igor Kotenko (2017). "Enhancement of probabilistic attack graphs for accurate cyber security monitoring". In: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, pp. 1–6.
- Kandias, Miltiadis et al. (2017). "Stress level detection via OSN usage pattern and chronicity analysis: An OSINT threat intelligence module". In: Computers & Security 69, pp. 3–17.
- Khandpur, Rupinder Paul et al. (2017). "Crowdsourcing cybersecurity: Cyber attack detection using social media". In: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, pp. 1049–1057.
- Lee, Kuo-Chan et al. (2017). "Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation". In: Soft Computing 21.11, pp. 2883–2896.
- Liu, Ruyue et al. (2017). "A Research and Analysis Method of Open Source Threat Intelligence Data". In: International Conference of Pioneering Computer Scientists, Engineers and Educators. Springer, pp. 352–363.
- Polatidis, Nikolaos, Elias Pimenidis, Michalis Pavlidis and Haralambos Mouratidis (2017). "Recommender systems meeting security: From product recommendation to cyber- attack prediction". In: International Conference on Engineering Applications of Neural Networks. Springer, pp. 508–519.
- Price-Williams, Matthew, Nick Heard and Melissa Turcotte (2017). "Detecting periodic subsequences in cyber security data". In: 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, pp. 84–90.
- Qamar, Sara et al. (2017). "Data-driven analytics for cyber- threat intelligence and information sharing". In: Computers & Security 67, pp. 35–58.
- Ślezak, Dominik et al. (2017). "Scalable cyber-security analytics with a new summary-based approximate query engine". In: 2017 IEEE International Conference on Big Data (Big Data). IEEE, pp. 1840–1849.
- Stine, Ian et al. (2017). "A cyber risk scoring system for medical devices". In: International Journal of Critical Infrastructure Protection 19, pp. 32–46.
- Teoh, TT et al. (2017). "Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data". In: 2017 13th International Conference on

Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD). IEEE, pp. 2080–2083.

- Wagner, Thomas D et al. (2017). "Towards an Anonymity Supported Platform for Shared Cyber Threat Intelligence". In: International Conference on Risks and Security of Internet and Systems. Springer, pp. 175–183.
- Yaseen, Amer Atta and Mireille Bayart (2017). "Cyber-attack detection with fault accommodation based on intelligent generalized predictive control". In: IFAC-PapersOnLine 50.1, pp. 2601–2608.
- Aditya, K, Slawomir Grzonkowski and Nhien-An Le-Khac (2018). "Riskwriter: Predicting cyber risk of an enterprise". In: International Conference on Information Systems Security. Springer, pp. 88–106.
- Almohannadi, Hamad et al. (2018). "Cyber threat intelligence from honeypot data using elasticsearch". In: 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, pp. 900–906.
- Araujo, Frederico et al. (2018). "Cross-Stack Threat Sensing for Cyber Security and Resilience". In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). IEEE, pp. 18–21.
- Barboni, Angelo, Francesca Boem and Thomas Parisini (2018). "Model-based detection of cyber-attacks in networked MPC-based control systems". In: IFAC-PapersOnLine 51.24, pp. 963–968.
- Böhm, Fabian, Florian Menges and Günther Pernul (2018). "Graph-based visual analytics for cyber threat intelligence". In: Cybersecurity 1.1, p. 16.
- Cho, Hyeisun et al. (2018). "Method of Quantification of Cyber Threat Based on Indicator of Compromise". In: 2018 International Conference on Platform Technology and Service (PlatCon). IEEE, pp. 1–6.
- Ghazi, Yumna et al. (2018). "A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources". In: 2018 International Conference on Frontiers of Information Technology (FIT). IEEE, pp. 129–134.
- Gokaraju, Balakrishna et al. (2018). "Identification of spatio- temporal patterns in cyber security for detecting the signature identity of hacker". In: SoutheastCon 2018. IEEE, pp. 1–5.
- Gonzalez-Granadillo, G et al. (2018). "Dynamic risk management response system to handle cyber threats". In: Future Generation Computer Systems 83, pp. 535–552.
- Gschwandtner, Mathias et al. (2018). "Integrating threat intelligence to enhance an organization's information security management". In: Proceedings of the 13th International Conference on Availability, Reliability and Security, pp. 1–8.
- Guerrero-Higueras, Ángel Manuel, Noemi DeCastro-Garcia and Vicente Matellan (2018). "Detection of Cyber-attacks to indoor real time localization systems for autonomous robots". In: Robotics and Autonomous Systems 99, pp. 75– 83.
- Haughey, Hamish et al. (2018). "Adaptive traffic fingerprinting for darknet threat intelligence". In: Cyber Threat Intelligence. Springer, pp. 193–217.
- Iqbal, Zafar, Zahid Anwar and Rafia Mumtaz (2018). "STIXGEN-A Novel Framework for Automatic Generation of Structured Cyber Threat Information". In: 2018 International Conference on Frontiers of Information Technology (FIT). IEEE, pp. 241–246.
- Kim, Eunsoo et al. (2018). "CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules". In: Proceedings of the 13th International Conference on Future Internet Technologies, pp. 1–5.
- Kim, Nakhyun et al. (2018). "Study of Natural Language Processing for Collecting Cyber Threat Intelligence Using SyntaxNet". In: International Symposium of Information and Internet Technology. Springer, pp. 10–18.
- Kotenko, Igor et al. (2018). "AI-and metrics-based vulnerability-centric cyber security assessment and countermeasure selection". In: Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, pp. 101–130.

- Lee, Chanyoung, Ho Bin Yim and Poong Hyun Seong (2018). "Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept". In: Annals of Nuclear Energy 112, pp. 646–654.
- Moskal, Stephen, Shanchieh Jay Yang and Michael E Kuhl (2018). "Extracting and evaluating similar and unique cyber attack strategies from intrusion alerts". In: 2018 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, pp. 49–54.
- Pitropakis, Nikolaos et al. (2018). "An enhanced cyber attack attribution framework". In: International Conference on Trust and Privacy in Digital Business. Springer, pp. 213– 228.
- Prabhu, Vinayak et al. (2018). "Towards Data-Driven Cyber Attack Damage and Vulnerability Estimation for Manufacturing Enterprises". In: International Conference on Remote Engineering and Virtual Instrumentation. Springer, pp. 333– 343.
- Radanliev, Petar et al. (2018). "Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance". In:
- Shu, Kai et al. (2018). "Understanding cyber attack behaviors with sentiment information on social media". In: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. Springer, pp. 377–388.
- Smith, Matthew David and M Elisabeth Paté-Cornell (2018). "Cyber risk analysis for a smart grid: how smart is smart enough? a multiarmed bandit approach to cyber security investment". In: IEEE Transactions on Engineering Management 65.3, pp. 434–447.
- Vinayakumar, R, Prabaharan Poornachandran and KP Soman (2018). "Scalable framework for cyber threat situational awareness based on domain name systems data analysis". In: Big data in engineering applications. Springer, pp. 113– 142.
- Wang, Junshe et al. (2018). "Network attack prediction method based on threat intelligence". In: International Conference on Cloud Computing and Security. Springer, pp. 151–160.
- Zieger, Andrej, Felix Freiling and Klaus-Peter Kossakowski (2018). "The β-time-to-compromise metric for practical cyber security risk estimation". In: 2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF). IEEE, pp. 115–133.
- Bo, Tao et al. (2019). "TOM: A Threat Operating Model for Early Warning of Cyber Security Threats". In: International Conference on Advanced Data Mining and Applications. Springer, pp. 696–711.
- Doynikova, Elena, Andrey Fedorchenko and Igor Kotenko (2019). "Ontology of metrics for cyber security assessment". In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1–8.
- Dragos, Valentina et al. (2019). "Entropy-Based Metrics for URREF Criteria to Assess Uncertainty in Bayesian Networks for Cyber Threat Detection". In: 2019 22th International Conference on Information Fusion (FUSION). IEEE, pp. 1–8.
- Gautam, Apurv Singh, Yamini Gahlot and Pooja Kamat (2019). "Hacker Forum Exploit and Classification for Proactive Cyber Threat Intelligence". In: International Conference on Inventive Computation Technologies. Springer, pp. 279–285.
- Kannavara, Raghudeep et al. (2019). "A threat intelligence tool for the security development lifecycle". In: Proceedings of the 12th Innovations on Software Engineering Conference (formerly known as India Software Engineering Conference), pp. 1–5.
- Keim, Yansi and AK Mohapatra (2019). "Cyber threat intelligence framework using advanced malware forensics". In: International Journal of Information Technology, pp. 1–10.

- Al-khateeb, Samer and Nitin Agarwal (2019). "Social cyber forensics: leveraging open source information and social network analysis to advance cyber security informatics". In: Computational and Mathematical Organization Theory, pp. 1–19.
- Li, Yi-Fan et al. (2019). "Multistream classification for cyber threat data with heterogeneous feature space". In: The World Wide Web Conference, pp. 2992–2998.
- Marukhlenko, AL, AV Plugatarev and DO Bobyntsev (2019). "Complex Evaluation of Information Security of an Object with the Application of a Mathematical Model for Calculation of Risk Indicators". In: International Russian Automation Conference. Springer, pp. 771–778.
- Merino, Tim et al. (2019). "Expansion of cyber attack data from unbalanced datasets using generative adversarial networks". In: International Conference on Software Engi- neering Research, Management and Applications. Springer, pp. 131–145.
- Milajerdi, Sadegh M et al. (2019). "Poirot: Aligning attack behavior with kernel audit records for cyber threat hunting". In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1795–1812.
- Milošević, Jezdimir, Henrik Sandberg and Karl Henrik Johansson (2019). "Estimating the impact of cyber-attack strategies for stochastic networked control systems". In: IEEE Transactions on Control of Network Systems 7.2, pp. 747–757
- Mokaddem, Sami et al. (2019). "Taxonomy driven indicator scoring in MISP threat intelligence platforms". In: arXiv preprint arXiv:1902.03914.
- Mukhopadhyay, Arunabha et al. (2019). "Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance". In: Information Systems Frontiers 21.5, pp. 997–1018.
- Noor, Umara et al. (2019). "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories". In: Future Generation Computer Systems 95, pp. 467–487.
- Okutan, Ahmet and Shanchieh Jay Yang (2019). "ASSERT: attack synthesis and separation with entropy redistribution towards predictive cyber defense". In: Cybersecurity 2.1, pp. 1–18.
- Papastergiou, Spyridon, Haralambos Mouratidis and Eleni- Maria Kalogeraki (2019). "Cyber security incident handling, warning and response system for the european critical information infrastructures (cybersane)". In: International Conference on Engineering Applications of Neural Networks. Springer, pp. 476–487.
- Pour, Morteza Safaei et al. (2019). "Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns". In: Digital Investigation 28, S40–S49.
- Riesco, Raúl and Víctor A Villagrá (2019). "Leveraging cyber threat intelligence for a dynamic risk framework". In: International Journal of Information Security 18.6, pp. 715–739.
- Rijswijk-Deij, Roland van et al. (2019). "Privacy-conscious threat intelligence using DNSBLoom". In: 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, pp. 98–106.
- Simran, K et al. (2019). "Deep Learning Approach for Enhanced Cyber Threat Indicators in Twitter Stream". In: International Symposium on Security in Computing and Communication. Springer, pp. 135–145.
- Sliva, Amy, Kai Shu and Huan Liu (2019). "Using social media to understand cyber attack behavior". In: International Conference on Applied Human Factors and Ergonomics. Springer, pp. 636–645.
- Subroto, Athor and Andri Apriyana (2019). "Cyber risk prediction through social media big data analytics and statistical machine learning". In: Journal of Big Data 6.1, pp. 1–19.
- Tonn, Gina et al. (2019). "Cyber risk and insurance for transportation infrastructure". In: Transport policy 79, pp. 103–114.

- Trivedi, Tarun et al. (2019). "Threat Intelligence Analysis of Onion Websites Using Sublinks and Keywords". In: Emerging Technologies in Data Mining and Information Security. Springer, pp. 567–578.
- Ullah, Sharif et al. (2019). "Cyber Threat Analysis Based on Characterizing Adversarial Behavior for Energy Delivery System". In: International Conference on Security and Privacy in Communication Systems. Springer, pp. 146–160.
- Ustebay, Serpil, Zeynep Turgut and M Ali Aydin (2019). "Cyber Attack Detection by Using Neural Network Approaches: Shallow Neural Network, Deep Neural Network and AutoEncoder". In: International Conference on Com- puter Networks. Springer, pp. 144–155.
- Vielberth, Manfred, Florian Menges and Günther Pernul (2019). "Human-as-a-security-sensor for harvesting threat intelligence". In: Cybersecurity 2.1, pp. 1–15.
- Vinayakumar, R, KP Soman, et al. (2019). "Deep learning framework for cyber threat situational awareness based on email and url data analysis". In: Cybersecurity and Secure Information Systems. Springer, pp. 87–124.
- Wang, Huaizhi et al. (2019). "Deep learning aided interval state prediction for improving cyber security in energy internet". In: Energy 174, pp. 1292–1304.
- Wangen, Gaute (2019). "Quantifying and Analyzing Information Security Risk from Incident Data". In: International Workshop on Graphical Models for Security. Springer, pp. 129–154.
- Yang, Wenzhuo and Kwok-Yan Lam (2019). "Automated Cyber Threat Intelligence Reports Classification for Early Warning of Cyber Attacks in Next Generation SOC". In: International Conference on Information and Communications Security. Springer, pp. 145–164.
- Zhang, Hongbin et al. (2019). "Network attack prediction method based on threat intelligence for IoT". In: Multimedia Tools and Applications 78.21, pp. 30257–30270.
- Almukaynizi, Mohammed et al. (2020). "A Logic Programming Approach to Predict Enterprise-Targeted Cyberattacks". In: Data Science in Cybersecurity and Cyberthreat Intelligence. Springer, pp. 13–32.
- Barrère, Martın et al. (2020). "Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies". In: Journal of Information Security and Applications 52, p. 102471.
- Chen, Scarlett, Zhe Wu and Panagiotis D Christofides (2020). "Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control". In: Computers & Chemical Engineering, p. 106806.
- Evangelou, Marina and Niall M Adams (2020). "An anomaly detection framework for cyber-security data". In: Computers & Security 97, p. 101941.
- Facchinetti, Silvia, Paolo Giudici and Silvia Angela Osmetti (2020). "Cyber risk measurement with ordinal data". In: Statistical Methods & Applications 29.1, pp. 173–185.
- Figueira, Pedro Tubıo, Cristina López Bravo and José Luis Rivas López (2020). "Improving information security risk analysis by including threat-occurrence predictive models". In: Computers & Security 88, p. 101609.
- Huang, Linan and Quanyan Zhu (2020). "A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems". In: Computers & Security 89, p. 101660.
- Khosravi, Mehran and Behrouz Tork Ladani (2020). "Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection". In: IEEE Access 8, pp. 162642–162656.
- Kour, Ravdeep, Adithya Thaduri and Ramin Karim (2020). "Predictive model for multistage cyber-attack simulation". In: International Journal of System Assurance Engineering and Management 11.3, pp. 600–613.
- Krisper, Michael, Jürgen Dobaj and Georg Macher (2020). "Assessing Risk Estimations for Cyber-Security Using Expert Judgment". In: European Conference on Software Process Improvement. Springer, pp. 120–134.

- Liao, Yi-Ching (2020). "Quantitative Information Security Vulnerability Assessment for Norwegian Critical Infrastructure". In: International Conference on Critical Information Infrastructures Security. Springer, pp. 31–43.
- Luh, Robert and Sebastian Schrittwieser (2020). "Advanced threat intelligence: detection and classification of anomalous behavior in system processes". In: e & i Elektrotechnik und Informationstechnik 137.1, pp. 38–44.
- Marin, Ericsson, Mohammed Almukaynizi and Paulo Shakarian (2020). "Inductive and deductive reasoning to assist in cyber-attack prediction". In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, pp. 0262–0268.
- Al-Mohannadi, Hamad, Irfan Awan and Jassim Al Hamar (2020). "Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence". In: Service Oriented Computing and Applications, pp. 1–13.
- Mohasseb, Alaa et al. (2020). "Cyber security incidents analysis and classification in a case study of Korean enterprises". In: Knowledge and Information Systems.
- Polatidis, Nikolaos, Elias Pimenidis, Michalis Pavlidis, Spyridon Papastergiou, et al. (2020). "From product recommendation to cyber-attack prediction: generating attack graphs and predicting future attacks". In: Evolving Systems, pp. 1– 12.
- Rahman, Md Anisur, Yeslam Al-Saggaf and Tanveer Zia (2020). "A Data Mining Framework to Predict Cyber Attack for Cyber Security". In: The 15th IEEE Conference on Industrial Electronics and Applications (ICIEA2020). IEEE Xplore.
- Tundis, Andrea, Samuel Ruppert and Max Mühlhäuser (2020). "On the Automated Assessment of Open-Source Cyber Threat Intelligence Sources". In: International Conference on Computational Science. Springer, pp. 453–467.
- Uyheng, Joshua et al. (2020). "Interoperable pipelines for social cyber-security: Assessing Twitter information Operations during NATO Trident Juncture 2018". In: Computational and Mathematical Organization Theory 26.4, pp. 465–483.
- Zhao, Jun et al. (2020). "TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data". In: Computers & Security, p. 101867.

References

1. Madnick, S. How Do You Prepare for the Unexpected Cyber Attack? *SSRN Electron. J.* **2020**. [CrossRef]
2. Anderson, R.; Böhme, R.; Clayton, R.; Moore, T. Security Economics and the Internal Market. Available online: https://www.enisa.europa.eu/publications/archive/economics-sec/ (accessed on 23 March 2021).
3. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report EBSE-2007-01, Joint Report; Keele University: Keele, UK; University of Durham: Durham, UK, 2007.
4. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [CrossRef]
5. Lea, D.; Bradbery, J. Oxford Advanced Learner's Dictionary. 2021. Available online: https://www.oxfordlearnersdictionaries.com/definition/english/indicator (accessed on 22 April 2021).
6. Pfleeger, S.L.; Caputo, D.D. Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Comput. Secur.* **2012**, *31*, 597–611. [CrossRef]
7. Brown, S.; Gommers, J.; Serrano, O. From Cyber Security Information Sharing to Threat Management. *WISCS '15: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*; Association for Computing Machinery: New York, NY, USA, 2015; pp. 43–49.
8. McMillan, R. Definition: Threat Intelligence. Available online: https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf (accessed on 26 March 2021).
9. Tounsi, W.; Rais, H. A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
10. Chismon, D.; Ruks, M. Threat Intelligence: Collecting, Analysing, Evaluating. Available online: https://informationsecurity.report/whitepapers/threat-intelligence-collecting-analysing-evaluating/10 (accessed on 26 March 2021).
11. Mateski, M.; Trevino, C.M.; Veitch, C.K.; Michalski, J.; Harris, J.M.; Maruoka, S.; Frye, J. Cyber Threat Metrics. Available online: https://fas.org/irp/eprint/metrics.pdf (accessed on 26 March 2021).
12. Wang, A.J.A. Information Security Models and Metrics. In Proceedings of the 43rd Annual Southeast Regional Conference, (ACM-SE 43), Kennesaw, GA, 18 –20 March 2005; pp. 178–184.

13. Herrmann, D.S. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*, 1st ed.; Auerbach Publications: Boston, MA, USA, 2007.
14. Humayun, M.; Niazi, M.; Jhanjhi, N.Z.; Alshayeb, M.; Mahmood, S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
15. Grajeda, C.; Breitinger, F.; Baggili, I. Availability of Datasets for Digital Forensics—And What is Missing. *Digit. Investig.* **2017**, *22*, S94–S105. [CrossRef]
16. Zheng, M.; Robbins, H.; Chai, Z.; Thapa, P.; Moore, T. Cybersecurity Research Datasets: Taxonomy and Empirical Analysis. In Proceedings of the 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET'18), Baltimore, MD, USA, 13 August 2018.
17. Griffioen, H.; Booij, T.; Doerr, C. Quality Evaluation of Cyber Threat Intelligence Feeds. In Proceedings of the 18th International Conference on Applied Cryptography and Network Security (ACNS'20), Rome, Italy, 19–22 October 2020; pp. 277–296.
18. Tundis, A.; Ruppert, S.; Mühlhäuser, M. On the Automated Assessment of Open-Source Cyber Threat Intelligence Sources. In Proceedings of the 20th International Conference on Computational Science (ICCS'20), Amsterdam, The Netherlands, 3–5 June 2020; pp. 453–467.
19. Pendleton, M.; Garcia-Lebron, R.; Cho, J.H.; Xu, S. A Survey on Systems Security Metrics. *ACM Comput. Surv. CSUR* **2016**, *49*, 1–35. [CrossRef]
20. Cadena, A.; Gualoto, F.; Fuertes, W.; Tello-Oquendo, L.; Andrade, R.; Tapia Leon, F.; Torres, J. Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study. In *Smart Innovation, Systems and Technologies*; Springer Nature Singapore Private Limited: Singapore, Singapore, 2020; pp. 507–519. [CrossRef]
21. Husák, M.; Komárková, J.; Bou-Harb, E.; Čeleda, P. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 640–660. [CrossRef]
22. Sriavstava, R.; Singh, P.; Chhabra, H., Review on Cyber Security Intrusion Detection: Using Methods of Machine Learning and Data Mining. In *Internet of Things and Big Data Applications: Recent Advances and Challenges*; Springer: Cham, Switzerland, 2020; pp. 121–132. [CrossRef]
23. Sun, N.; Zhang, J.; Rimba, P.; Gao, S.; Zhang, L.Y.; Xiang, Y. Data-Driven Cybersecurity Incident Prediction: A Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1744–1772. [CrossRef]
24. Laube, S.; Böhme, R. Strategic Aspects of Cyber Risk Information Sharing. *ACM Comput. Surv. CSUR* **2017**, *50*, 1–36. [CrossRef]
25. Diesch, R.; Krcmar, H. SoK: Linking Information Security Metrics to Management Success Factors. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20), Dublin, Ireland, 25–28 August 2020; pp. 1–10.
26. Kotenko, I.; Doynikova, E.; Chechulin, A.; Fedorchenko, A., AI- and Metrics-Based Vulnerability-Centric Cyber Security Assessment and Countermeasure Selection. In *Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach*; Springer: Cham, Switzerland, 2018; pp. 101–130. [CrossRef]
27. Gheyas, I.A.; Abdallah, A.E. Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis. *Big Data Anal.* **2016**, *1*, 1–29. [CrossRef]
28. Keim, Y.; Mohapatra, A.K. Cyber Threat Intelligence Framework Using Advanced Malware Forensics. *Int. J. Inf. Technol.* **2019**, 1–10. [CrossRef]
29. Samtani, S.; Abate, M.; Benjamin, V.; Li, W., Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 135–154. [CrossRef]
30. Chockalingam, S.; Pieters, W.; Teixeira, A.; van Gelder, P. Bayesian Network Models in Cyber Security: A Systematic Review. In Proceedings of the 22nd Nordic Conference on Secure IT Systems (NordSec'17), Tartu, Estonia, 8–10 November 2017; pp. 105–122.
31. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic Mapping Studies in Software Engineering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE'08), Bari, Italy, 26–27 June 2008; pp. 1–10.
32. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from Applying the Systematic Literature Review Process within the Software Engineering Domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [CrossRef]
33. Wohlin, C. Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE'14), London, UK, 13–14 May 2014; pp. 1–10.
34. Wieringa, R.; Maiden, N.; Mead, N.; Rolland, C. Requirements Engineering Paper classification and Evaluation Criteria: A Proposal and a Discussion. *Requir. Eng.* **2006**, *11*, 102–107. [CrossRef]
35. The MITRE Corporation. Common Weakness Enumeration (CWE). 2021. Available online: https://cwe.mitre.org/ (accessed on 22 April 2021).
36. Meland, P.H.; Tokas, S.; Erdogan, G.; Bernsmed, K.; Omerovic, Cyber Security Indicators Mapping Scheme and Result. 2021. Available online: https://doi.org/10.5281/zenodo.4639585 (accessed on 19 March 2021).
37. Erdogan, G.; Gonzalez, A.; Refsdal, A.; Seehusen, F. A Method for Developing Algorithms for Assessing Cyber-Risk Cost. In Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS'17), Prague, Czech Republic, 25–29 July 2017; pp. 192–199.
38. Moore, T.; Kenneally, E.; Collett, M.; Thapa, P. Valuing Cybersecurity Research Datasets. In Proceedings of the 18th Workshop on the Economics of Information Security (WEIS'19), Boston, MA, USA, 3–4 June 2019; pp. 1–27.

39. Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber Threat Intelligence Sharing: Survey and Research Directions. *Comput. Secur.* **2019**, *87*, 101589. [CrossRef]
40. Barnum, S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). *Mitre Corp.* **2012**, *11*, 1–22.
41. Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. *Electronics* **2020**, *9*, 824. [CrossRef]
42. Bromander, S.; Muller, L.P.; Eian, M.; Jøsang, A. Examining the "Known Truths" in Cyber Threat Intelligence–The Case of STIX. In Proceedings of the 15th International Conference on Cyber Warfare and Security, Norfolk, VA, USA, 12–13 March 2020; p. 493-XII.
43. Bromander, S.; Swimmer, M.; Muller, L.; Jøsang, A.; Eian, M.; Skjøtskift, G.; Borg, F. Investigating Sharing of Cyber Threat Intelligence and Proposing a New Data Model for Enabling Automation in Knowledge Representation and Exchange. *Digit. Threat. Res. Pract.* **2021**. [CrossRef]
44. Mavroeidis, V.; Bromander, S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC'17), Athens, Greece, 11–13 September 2017; pp. 91–98.
45. Garousi, V.; Felderer, M.; Mäntylä, M.V. The Need for Multivocal Literature Reviews in Software Engineering: Complementing Systematic Literature Reviews with Grey Literature. In Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering (EASE'16), Limerick, Ireland, 1–3 June 2016; pp. 1–6.