informatics

Article

The Evolution of Digital Security by Design Using Temporal Network Analysis

Lowri Williams *, Hamza Khan and Pete Burnap

School of Computer Science & Informatics, Cardiff University, Cardiff CF24 4AG, UK;
khanh29@cardiff.ac.uk (H.K.); burnapp@cardiff.ac.uk (P.B.)
* Correspondence: williamsl10@cardiff.ac.uk

Abstract: Digital Security by Design (DSbD) is an initiative supported by the UK government aimed at transforming digital technology to deliver necessary digital resilience and prosperity across the UK. As emerging challenges in the field of digital security evolve, it becomes essential to explore how entities involved in DSbD interact and change over time. Understanding these dynamic relationships can provide crucial insights for the development and improvement of security practices. This paper presents a data-driven analysis of the evolving landscape of DSbD from 2019 to 2024, gathering insights from textual documents referencing DSbD. Using a combination of text mining techniques and network analysis, a large corpus of textual documents was examined to identify key entities, including organisations, individuals, and the relationships between them. A network was then visualised to analyse the structural connections between these entities, revealing how key concepts and actors have evolved. The results and discussion demonstrate that the network analysis offers a unique advantage in tracking and visualising these evolving relationships, providing insights into shifts in focus, emerging trends, and changes in technological adoption over time. For example, a notable finding from the analysis is the substantial increase in node relationships associated with Artificial Intelligence (AI). We hypothesise that this surge reflects the growing integration of AI into digital security strategies, driven by the need for more adaptive and autonomous solutions to tackle evolving cyber threats, as well as the rapid introduction of new AI tools to the market and their swift adoption across various industries. By mapping such connections, such results are useful, helping practitioners and researchers recognise new security demands and adjust strategies to better respond to the evolving landscape of DSbD.

Keywords: temporal network analysis; digital security by design; security by design; natural language processing; text mining

check for updates

Received: 5 November 2024
Revised: 14 January 2025
Accepted: 15 January 2025
Published: 17 January 2025

Citation: Williams, L.; Khan, H.; Burnap, P. The Evolution of Digital Security by Design Using Temporal Network Analysis. *Informatics* **2025**, *12*, 8. https://doi.org/10.3390/informatics12010008

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The landscape of digital security research is marked by a growing recognition of the need for proactive, foundational security approaches that integrate protective measures at every layer of digital infrastructure. Security by Design (SbD) is a longstanding concept focused on embedding security throughout the development of systems and technologies, making it integral to product design and minimising vulnerabilities [1–3]. SbD emphasises principles such as least privilege, defence in depth, and regular threat assessments, providing a framework that has been widely adopted across sectors [2]. However, as cyber threats become more sophisticated and pervasive, a broader, more systemic approach is needed to address inherent architectural vulnerabilities that SbD alone may not fully mitigate.

To address these challenges, the Digital Security by Design (DSbD) [4] initiative, launched by the UK government, aims to redesign digital systems from the ground up to make them inherently resilient to cyber threats [5]. DSbD focuses on creating secure hardware and software infrastructures that proactively mitigate vulnerabilities at the architectural level, with projects like the Arm Morello prototype exemplifying DSbD's commitment to secure hardware development [6]. This initiative reflects an increasing recognition that secure-by-default digital environments are necessary for comprehensive security, particularly in complex systems and critical infrastructure where traditional SbD approaches may leave certain vulnerabilities exposed [7].

Emerging technologies such as Artificial Intelligence (AI) and cloud computing have further complicated the digital security landscape, introducing both new capabilities and potential vulnerabilities [8]. AI in cybersecurity, for instance, has transformed threat detection and response through predictive modelling and anomaly detection, but its integration also brings risks related to data integrity and adversarial attacks [9]. As organisations and governments adopt these advanced technologies, there is an increased need for security frameworks that can adapt to rapid technological changes and the evolving threat landscape.

It is also essential to understand not only the technological advancements but also the complex network of relationships and collaborations that drive these developments. The DSbD landscape is composed of a diverse array of stakeholders, including governmental research bodies like UK Research and Innovation (UKRI) [10], security organisations such as the National Cyber Security Centre (NCSC) [11], private sector companies working on secure hardware like Capability Hardware Enhanced RISC Instructions (CHERI) [12], and academic researchers advancing AI-driven security techniques. Such entities interact and collaborate in dynamic ways, shaping the direction and impact of DSbD technologies. Over time, certain players and technologies may gain prominence within the network, reflecting shifts in focus, funding, and innovation efforts.

To gather insights into the forces driving digital security innovation at scale within the complex and broad DSbD ecosystem, automated techniques are essential to systematically collect and programmatically analyse relevant information from publicly available sources. In this case, this paper takes a data-driven approach to explore and analyse the changing DSbD landscape between 2019 and 2024 by leveraging large-scale text analysis techniques to extract key entities and relationships from a large corpus of online documents. Such information is then used in network analysis to visualise and quantify the evolution of this ecosystem, where entities (nodes) represent organisations, individuals, or technologies, while connections (edges) reflect collaborations, partnerships, or shared developments. By doing so, the patterns and trends that define the development of DSbD are uncovered, central players and collaborations are identified, and an understanding of how the digital security landscape has changed over time is provided.

One of the key advantages of network analysis is its scalability and ability to handle large datasets, making it an ideal method for monitoring and analysing the temporal evolution of the DSbD landscape. As new technologies emerge and relationships between entities shift, network analysis provides a dynamic view of how these interactions change over time. It can identify not only the most influential actors but also the rise and fall of specific technologies or organisations within the ecosystem. Additionally, centrality measures, such as degree centrality, can be employed to quantify the influence of specific nodes within the network, offering insights into the critical entities driving DSbD innovation.

The contributions of this paper include:

- A collection of online narratives and documents referencing DSbD between 2019 and 2024, including their metadata such as URLs, document titles, publication dates, and content.
- By combining large-scale data collection, entity extraction, relationship analysis, and temporal tracking, we provide insights into the evolution of DSbD. Our findings reveal how the landscape of digital security has transformed over time, the growing importance of certain entities, and the emergence of new technologies and collaborations. This knowledge is crucial for stakeholders looking to understand the key drivers of digital security innovation, anticipate future trends, and guide strategic decision-making.
- The pipeline developed in this study is designed to be scalable and dynamic. As more data is collected over time, the system can seamlessly ingest and process new information, allowing for continuous updates to the network visualisation. This ensures that the framework remains adaptable to ongoing developments in the DSbD landscape. Whether new entities emerge, relationships shift, or additional data sources become available, the pipeline can dynamically integrate these inputs, making it a tool for long-term monitoring and analysis of digital security trends.
- To enable interactive exploration and deeper understanding of the DSbD network, a dynamic, browser-based visualisation of the network is available. Such visualisations allow users to navigate through the network, hover over nodes to explore relationships, and filter by specific criteria to focus on particular entities or timeframes. The interactive nature of this interface allows stakeholders to gain deeper insights into how different organisations, individuals, and technologies are connected within the DSbD ecosystem, further making it a valuable tool for decision-making and research.

This study was designed as shown in Figure 1: (1) collect metadata (e.g., URLs, titles, publication dates) from online resources such as PDFs and web pages that contain references to target keywords, (2) collate a corpus of texts using collected metadata from search results, (3) automatically identify and classify key entities and actors involved in the DSbD landscape, (4) preprocess entities by filtering out those that contain non-alphanumeric characters, (5) extract entity relationships using a co-occurrence approach based on a five-sentence window, and (6) visualise and analyse chronological temporal networks.

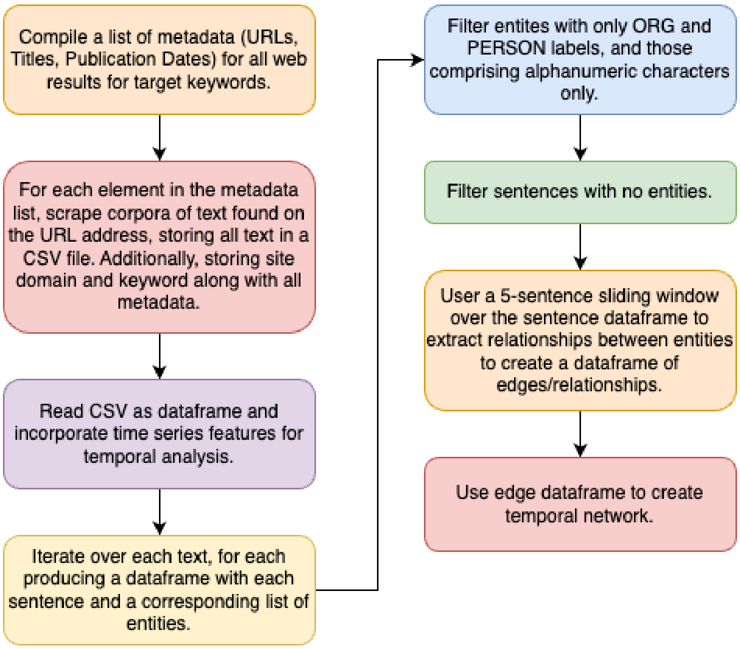

Compile a list of metadata (URLs, Titles, Publication Dates) for all web results for target keywords.
For each element in the metadata list, scrape corpora of text found on the URL address, storing all text in a CSV file. Additionally, storing site domain and keyword along with all metadata.
Read CSV as dataframe and incorporate time series features for temporal analysis.
Iterate over each text, for each producing a dataframe with each sentence and a corresponding list of entities.
Filter entites with only ORG and PERSON labels, and those comprising alphanumeric characters only.
Filter sentences with no entities.
User a 5-sentence sliding window over the sentence dataframe to extract relationships between entities to create a dataframe of edges/relationships.
Use edge dataframe to create temporal network.

Figure 1. An overview of the study design.

The remainder of this paper is structured as follows: Section 2 presents the related work, Section 3 discusses the collection of the texts used to support the experiments herein and the techniques used to prepare the data for visualising the networks, Section 4 presents and discusses the results, Section 5 concludes the paper and, finally, Section 6 discusses future work.

2. Related Work

While there has been significant research on digital security technologies, particularly in areas such as secure hardware architectures [13,14], AI in cybersecurity [15–17], and collaborative frameworks between academia and industry [18], there are very few directly comparable studies to the work presented here. Most existing research focuses on specific aspects of digital security without examining the holistic evolution of DSbD. Network analysis and text mining have been extensively applied in cybersecurity to process large volumes of unstructured data to extract actionable intelligence towards enhancing threat detection and risk management (e.g., [19–22]). However, the application of such techniques to track the temporal evolution of relationships within DSbD remains unexplored, highlighting the novelty of this study.

Radanliev [23] provides an in-depth review of the evolving landscape of digital security. It explores the increasing reliance on technologies such as IoT, AI, and cloud computing, emphasising the tension between user convenience and robust security measures. One of the key issues addressed is the design conflict between making systems easy to use and ensuring they are secure, particularly in the face of growing cyber threats. The study conducted a bibliometric analysis of records related to digital security from the Web of Science Core Collection and subsequently visualised emerging research categories and trends. It also incorporated thematic analysis and workshops to validate findings, providing a comprehensive view of the research landscape from 1997 to 2023. The study analysed clustering and keyword coupling to identify the key themes and objectives within digital security research, focusing on technological advancements like AI and quantum computing, as well as regulatory frameworks and sector-specific challenges. The paper concludes by providing actionable recommendations for stakeholders to navigate the evolving digital security environment, emphasising the need for adaptive strategies across sectors like healthcare, finance, and manufacturing.

While [23] offers a broad review of digital security by using bibliometric analysis to map general trends and themes across technologies and sectors, this study emphasises a data-driven, temporal analysis within the DSbD ecosystem, exploring how relationships and entities evolve within this ecosystem. Rather than focusing primarily on a wide range of technologies and regulatory themes, this study hones in on specific interactions, interdependencies, and dynamics within DSbD, examining the relationships among various entities. Here, network analysis is applied to map such interactions and relationships, capturing and visualising complex, multi-level relationships among DSbD entities, revealing clusters, influential entities, and emerging patterns. Such an approach allows the construction of a detailed, ecosystem-level view of DSbD, providing insights that are not limited to static trends but instead highlight the dynamics and shifts within the DSbD landscape over time.

Saqr [24] provides a comprehensive overview of temporal network analysis, which has emerged as a distinct field, integrating both relational and temporal dimensions to model dynamic phenomena such as information spread and viral trends [25]. Unlike static social networks, which represent connections as constant, temporal networks capture the dynamic nature of relationships by representing edges as emerging and dissolving over time, as edges have defined start and end times, ensuring unidirectional, time-restricted paths. Although temporal network analysis has not been investigated in the context of understanding the evolution of DSbD, it has been extensively employed to investigate the transformation of topics over time across various domains. For example, recent studies have applied such methods to analyse progression and shifts in research focus and the emergence of new subfields in the field of computational economics [26]. Others have applied temporal network analysis to emphasise the importance of understanding the evolutionary relationships among scientific topics to inform strategic decision-making in research and development [27]. Moreover, temporal network analysis has been used to trace topic transitions in social media platforms, such as Twitter [28]. Lastly, Zhang and Lauw [29] explore the time evolution of topics in temporally accumulative corpora to enhance the understanding of topic evolution in documents.

3. Data Collection, Preparation, and Visualisation

3.1. Textual Corpus Formation

To collate online narratives surrounding DSbD, targeted search queries were constructed. To refine the search results, Google’s quotation operator (“‘ ”’) was utilised to ensure that only results containing the exact phrases such as “Digital Security by Design”, “DSbD”, and “Digital Security” were returned. We used Google as the primary search engine for document collection due to its ability to index a diverse range of publicly accessible sources, including government publications, academic articles, and industry reports. This approach ensured a broad and transparent dataset for analysis while focusing on capturing emerging trends and dynamic relationships within the DSbD landscape.

In addition to using quotation marks, the “site:” operator was employed to limit the search to specific domains, specifically ”.uk” and ”.eu”, which are relevant to the analysis of the DSbD initiative, particularly within Europe and the UK. To capture only updated content, the URL was further modified with the following time-bound parameter ”&tbs=cdr:1,cd_min:1/1/0”. This addition enabled the search engine to return the last updated date of the search results, a critical element for the subsequent temporal analysis.

After constructing the search URL, metadata such as URLs, web page titles, and last updated dates was crawled using Scrapy (version 2.11.2) [30], an open-source web crawling and scraping framework written in Python. Scrapy’s asynchronous nature improved the efficiency of the data collection pipeline, allowing data from numerous web pages to be collected simultaneously. The constructed search URLs were then used with the keywords mentioned above to gather metadata from Google search results that referenced DSbD. This included metadata from both web pages and PDF documents spanning from 2019 to 2024. From over 290 URLs, which represented the online documents referring to DSbD, the metadata and the textual content of each page were collected. The metadata and content were stored in a Comma-Separated Values (CSV) file, a text file that stores data in a table-structured format with commas separating values and newlines separating records. In this file, each row represented a single document, complete with its date, title, URL, and full text.

3.2. Textual Data Processing

The collected CSV was imported into a dataframe using Pandas (version 2.2.3) [31], an open-source data analysis and manipulation tool written in Python. In this dataframe, each row represented a scraped document. In addition to the basic metadata, the dataframe was enriched with time series features, including the year, month, and day of the publication date, enabling temporal analysis. This allowed the exploration of how discussions around DSbD evolved and identified significant periods of increased activity and key shifts in focus.

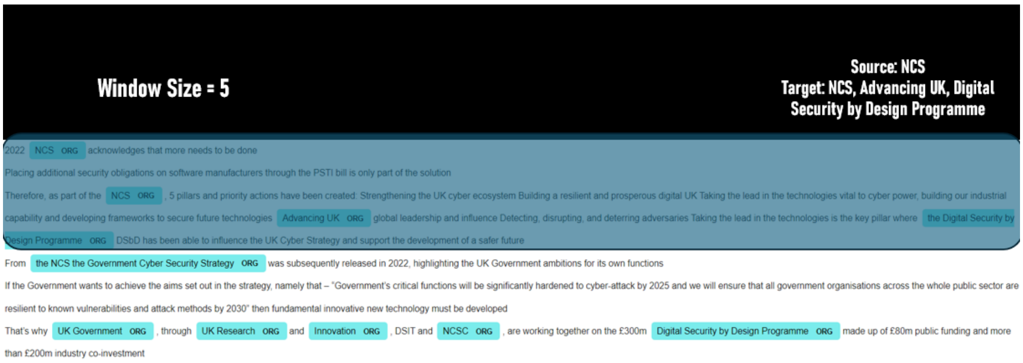
To automatically identify and classify key entities and actors involved in the DSbD landscape, such as organisations and individuals, Named Entity Recognition (NER) was performed. By performing NER using SpaCy (version 3.7.6) [32], a Python open-source library for Natural Language Processing (NLP) that can process large text corpora efficiently, it is possible to systematically extract important entities (labelled as "ORG" for organisations and "PERSON" for individuals) across a wide range of sources without manually combing through the data. SpaCy's largest English model, "en_core_web_lg", was selected for its balance between deep contextual extraction and speed. Moreover, NER helps streamline the identification of patterns, such as collaborations, partnerships, or key contributors to the discourse surrounding DSbD. Leveraging NER allows the construction of a comprehensive network of entities that are central to DSbD, allowing their interactions and relationships to be analysed over time. To ensure consistency and accuracy in the extract entities, those with non-alphanumeric characters or those starting with lowercase letters were removed.

3.3. Network Formation and Visualisation

To extract relationships between the entities extracted as part of NER, a sliding window approach was applied across the text corpus. By grouping consecutive sentences into windows of five, the relationships were inferred based on the co-occurrence of entities within the same window. The use of a sliding window approach with a small window size is a common approach to relationship extraction. The rationale behind this is that relationships between entities are often expressed within a local context, and a window of five sentences provides a balanced scope to capture relevant and meaningful co-occurrences without introducing excessive noise. A smaller window size may miss relationships that span multiple sentences, while a larger window size may include irrelevant information, diluting the relevance of the extracted relationships [33].

As shown in Figures 2 and 3, in each window, the relationships between the entities identified by the NER process are extracted. This relationship produces edges for the ontology based on textual proximity, or the closeness of terms or concepts within a text. When entities frequently appear near each other in such windows, it may suggest that they have a relationship or association. However, this relationship is based on co-occurrence and does not consider syntax, semantic, or contextual relationships between them.

This proximity-based method allows for the detection of implicit connections between entities, revealing patterns such as frequent collaborations or associations. This approach is domain-agnostic, as it does not rely on specific linguistic patterns but rather focuses on contextual proximity between entities. It also captures a broad range of relationships, from formal partnerships to incidental co-occurrences, providing a comprehensive view of the network of interactions.



Window Size = 5

Source: NCS
Target: NCS, Advancing UK, Digital Security by Design Programme

2022 NCS ORG acknowledges that more needs to be done

Placing additional security obligations on software manufacturers through the PSTI bill is only part of the solution

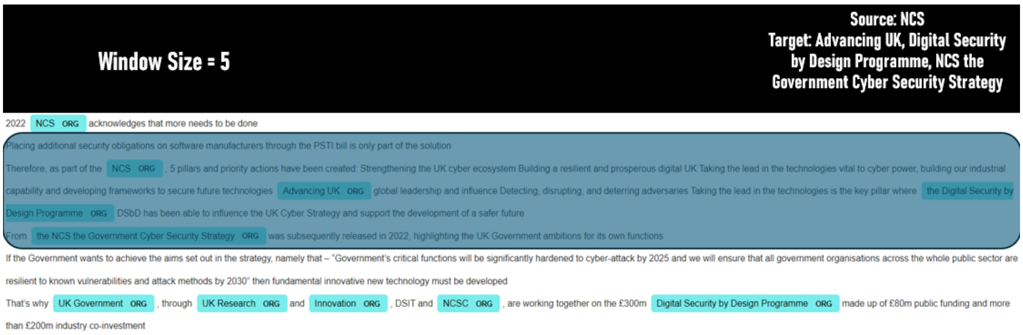
Therefore, as part of the NCS ORG , 5 pillars and priority actions have been created: Strengthening the UK cyber ecosystem Building a resilient and prosperous digital UK Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies Advancing UK ORG global leadership and influence Detecting, disrupting, and deterring adversaries Taking the lead in the technologies is the key pillar where the Digital Security by Design Programme ORG DSbD has been able to influence the UK Cyber Strategy and support the development of a safer future

From the NCS the Government Cyber Security Strategy ORG was subsequently released in 2022, highlighting the UK Government ambitions for its own functions

If the Government wants to achieve the aims set out in the strategy, namely that – "Government's critical functions will be significantly hardened to cyber-attack by 2025 and we will ensure that all government organisations across the whole public sector are resilient to known vulnerabilities and attack methods by 2030" then fundamental innovative new technology must be developed

That's why UK Government ORG , through UK Research ORG and Innovation ORG , DSIT and NCSC ORG , are working together on the £300m Digital Security by Design Programme ORG made up of £80m public funding and more than £200m industry co-investment

Figure 2. Extracting the first window of five sentences.



Window Size = 5

Source: NCS
Target: Advancing UK, Digital Security by Design Programme, NCS the Government Cyber Security Strategy

2022 NCS ORG acknowledges that more needs to be done

Placing additional security obligations on software manufacturers through the PSTI bill is only part of the solution

Therefore, as part of the NCS ORG , 5 pillars and priority actions have been created: Strengthening the UK cyber ecosystem Building a resilient and prosperous digital UK Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies Advancing UK ORG global leadership and influence Detecting, disrupting, and deterring adversaries Taking the lead in the technologies is the key pillar where the Digital Security by Design Programme ORG DSbD has been able to influence the UK Cyber Strategy and support the development of a safer future

From the NCS the Government Cyber Security Strategy ORG was subsequently released in 2022, highlighting the UK Government ambitions for its own functions

If the Government wants to achieve the aims set out in the strategy, namely that – "Government's critical functions will be significantly hardened to cyber-attack by 2025 and we will ensure that all government organisations across the whole public sector are resilient to known vulnerabilities and attack methods by 2030" then fundamental innovative new technology must be developed

That's why UK Government ORG , through UK Research ORG and Innovation ORG , DSIT and NCSC ORG , are working together on the £300m Digital Security by Design Programme ORG made up of £80m public funding and more than £200m industry co-investment

Figure 3. Extracting the second window of five sentences.

As a result of the relationship extraction process, Table 1 reports 13,316 unique entities, and 127,586 relationships were identified across the dataset. After removing duplicates, 19,489 unique relationships were retained. This means that each node has, on average, fewer than two direct relationships. These entities and relationships were then represented as a network, where nodes represent entities (organisations and people) and edges represent the inferred relationships between them.

Given the large size and its sparsity, visualising the network was essential for understanding the structure and dynamics of the DSbD landscape. To produce visualisations, Pyvis (version 0.3.2), a Python library that leverages vis.js to create interactive, browser-based visualisations, was used. The HTML-based visualisations generated by Pyvis allow for rich interactions with the network, enabling users to hover over nodes to explore their connections and groupings. Figure 4 illustrates how users can filter and search nodes based on various criteria, such as "AI", offering a deeper understanding of the relationships between key players and helping to uncover trends such as the concentration of influence around certain entities or the emergence of new connections.

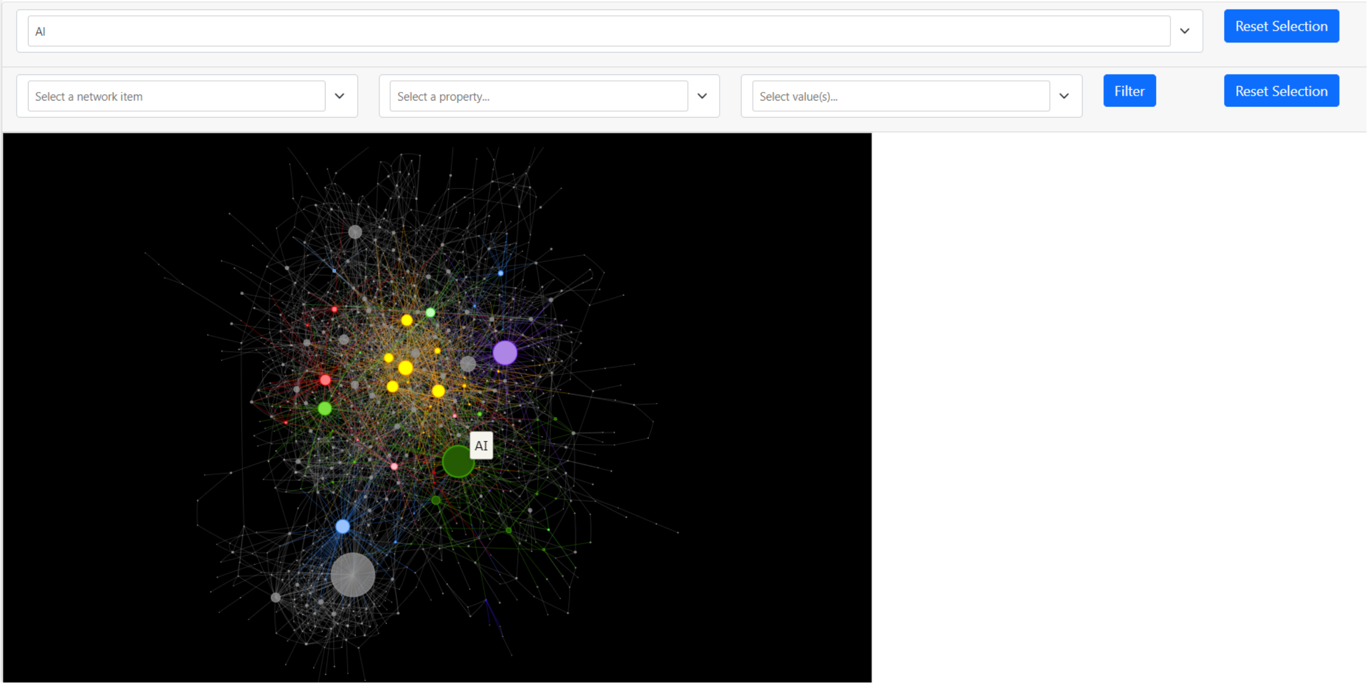


Figure 4. An interface to search for and filter network nodes.

Table 1. Distribution of nodes and relationships between 2019 and 2024.

Year	No. of Nodes	No. of Unique Edges
2019	1403	2237
2020	1759	2408
2021	1650	1916
2022	2106	2763
2023	2772	3576
2024	5284	7199

4. Results and Discussion

Due to the extensive size of the full network, only a filtered version is presented in this paper. Figure 5 displays the top 1000 nodes ranked by degree centrality, providing a more focused representation of the network's key components, whereas Figure 6a–f display the top 500 nodes in networks produced for data collected from 2019 to 2024.

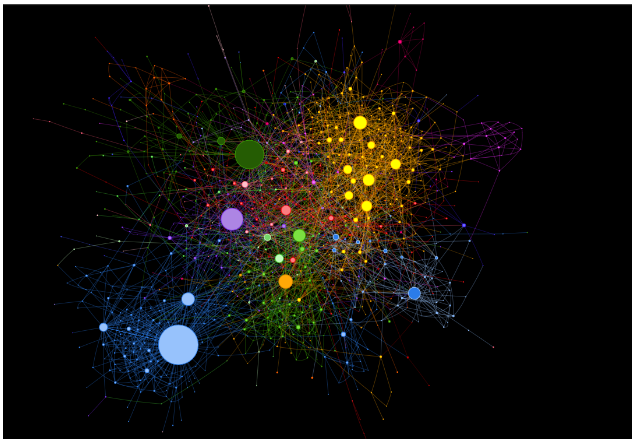


Figure 5. An excerpt of 1000 nodes from the non-temporal network.

To understand the network in Figure 5, as well as the forthcoming temporal networks, the importance of nodes may be investigated by measuring the centrality of the node degree, which measures the number of direct connections a node has in a network, indicating its immediate influence, and the centrality of closeness, which assesses how quickly a node can access all other nodes, reflecting its overall efficiency in spreading or receiving information.

Table 2 reports the node degree and closeness centrality for the non-temporal network. "Trust" (light blue node, bottom left in Figure 5) holds the highest degree centrality score (0.046), indicating its prominence in the network. This suggests that it is a crucial concept in the domain of Digital Security by Design, possibly due to its foundational role in security practices and regulatory frameworks. Other significant nodes include "NCSC" (0.015) and "AI" (0.014), reflecting the growing influence of AI in security-related discussions and the UK's active role in shaping digital security policies. Nodes such as "Digital Security" (0.012) exhibit lower centrality scores, indicating they are less prominent in the network but still relevant to its structure. This may imply that while these terms are essential to the discourse, more specific concepts like "Trust" and "AI" are currently driving the narrative in this context.

In addition to the above, the closeness centrality analysis illustrated that "Digital" (0.211), "AI" (0.210), "NCSC" (0.208), and "Cyber Security" (0.208) are the most central nodes in the network. This further highlights the growing importance of AI technologies and the UK's influence in digital security conversations. The centrality of "Digital" suggests that broader digital transformation efforts are also impacting the security landscape. Nodes like “Cyber Security” and “Morello” exhibit relatively high closeness centrality, highlighting their importance. “Morello”, for instance, may indicate a focus on innovative hardware security projects, while “Cyber Security” remains a core aspect of DSbD efforts.

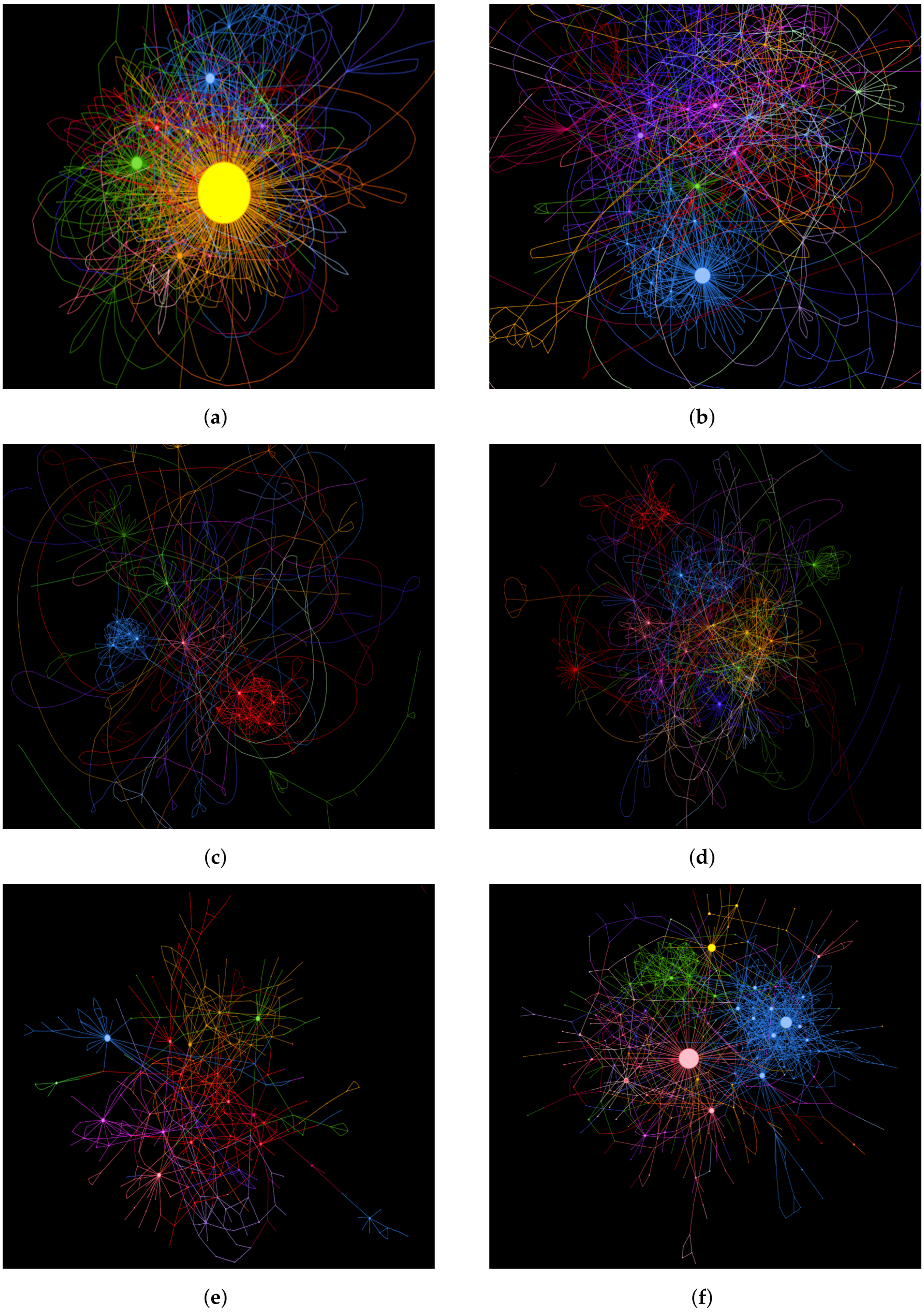


Figure 6. Network visualisations illustrating data from 2019 to 2024: (**a**) 2019, (**b**) 2020, (**c**) 2021, (**d**) 2022, (**e**) 2023, (**f**) 2024.

Edge weights represent the frequency of interactions between nodes, and therefore higher weights indicate more frequent relationships between those entities. The three most frequent relationships found in the network were “Department-UKRI”, “Google-Microsoft”, and “Board-Trust”. These strong connections suggest institutional collaboration in digital security efforts and the increasing role of tech giants like Google and Microsoft in shaping the security landscape. The prominence of "Trust" in its interactions with entities such as "CQC", "NHS", and "KPMG" may indicate a focus on healthcare security and the importance of trust frameworks in ensuring the safety of sensitive data in that sector. Similarly, "UKRI" appeared often with "Department", "HM Treasury", "CHERI", and "DSbD", which suggests significant governmental involvement in security innovation projects such as CHERI and the DSbD initiative.

Table 2. Node degree and closeness centrality scores from the non-temporal network.

Node	Closeness Centrality	Node	Degree Centrality
Digital	0.211	Trust	0.046
AI	0.210	NCSC	0.015
NCSC	0.208	Williams	0.014
Cyber Security	0.208	NHS	0.014
University	0.206	AI	0.014
UKRI	0.204	CHERI	0.013
Google	0.204	UKRI	0.013
Digital Security	0.203	Digital Security	0.012
Trust	0.203	Morello	0.010
Morello	0.202	Digital	0.010

The repeated appearance of "CHERI" with nodes like "Codasip", "Defence", "Morello", "UKRI", and "Rust" likely signals an ongoing focus on secure hardware architectures, particularly in defence and critical infrastructure sectors. These connections underscore the importance of collaboration between various entities in the development of secure and resilient systems.

Figure 6a–f visually illustrate the temporal networks between 2019 and 2024, with Table 1 revealing a significant growth in the number of relationships and entities over time from 2019 to 2024. Between these years, the number of edges increased from 14,343 to 45,609, while the number of nodes increased from 1403 to 5284 (see Table 1). This illustrates an expansion in publications and discussions surrounding the DSbD landscape, likely driven by increased research funding and the growing complexity of digital security challenges. The sharpest increase in both entities and relationships was observed in 2023–2024, which may correspond to heightened global interest in AI, cybersecurity, and advanced hardware solutions, as well as greater governmental and industry initiatives related to these areas. Tables 3 and 4 report the closeness centrality and degree centrality score for the top 10 nodes. Such scores reveal significant shifts in the network's structure and priorities.

In 2019, "Trust", illustrated by the yellow node located in the centre of the network in Figure 6a, emerged as the most dominant node with the highest scores in both metrics (degree: 0.265, closeness: 0.271), underscoring the significant focus on trust frameworks, especially in healthcare-related security, during this period. The prominence of "NHS" (degree: 0.057, closeness: 0.242) and "The Hillingdon Hospitals NHS Foundation Trust" (degree: 0.029, closeness: 0.239) further suggests that digital security discussions were heavily oriented toward the healthcare sector, likely in response to ongoing concerns about patient data security, regulatory compliance, and the need for robust security measures within national health systems. The presence of the "CQC" and the "NHS Foundation Trust" reinforces the idea that health institutions were key players in early Digital Security by Design initiatives. However, by 2024, these nodes will have largely decreased in influence, indicating a shift away from traditional governance and healthcare to technology-driven priorities.

Table 3. Node degree centrality scores between 2019 and 2024.

2019		2020	
Node	**Degree Centrality**	**Node**	**Degree Centrality**
Trust	0.265	Williams	0.087
NHS	0.057	ESRC	0.032
Board	0.047	EPSRC	0.027
The Hillingdon Hospitals NHS Foundation Trust	0.029	Digital	0.024
CQC	0.024	Cyber Security	0.017
UKRI	0.019	NCSC	0.017
Committee	0.018	Cardiff University	0.016
NHS Foundation Trust	0.016	Manchester	0.016
GP	0.014	University	0.014
Hillingdon Hospital	0.013	Twitter	0.013
2021		2022	
Node	**Degree Centrality**	**Node**	**Degree Centrality**
NCSC	0.073	NCSC	0.027
UKRI	0.055	SU Repository	0.020
National Cyber Strategy	0.048	SGN	0.017
Innovation	0.032	Bada	0.017
State	0.032	Morello	0.015
UK Research and Innovation	0.028	NCA	0.013
Department	0.027	Google	0.013
NCA	0.024	NCF	0.011
Industrial Strategy	0.023	Cyber Security	0.010
NCF	0.023	DCMS	0.009
2023		2024	
Node	**Degree Centrality**	**Node**	**Degree Centrality**
ITM	0.022	CHERI	0.050
BT	0.018	Digital Security	0.026
SGN	0.013	AI	0.024
AI	0.013	DSS	0.019
Lancaster University	0.011	Ofcom	0.015
Microsoft	0.011	TechWorks	0.014
NAV	0.011	UKRI	0.014
EU	0.009	Bank	0.013
Amazon	0.009	NHS	0.013
UKRI	0.009	Morello	0.012

Table 4. Node closeness centrality scores between 2019 and 2024.

2019		2020	
Node	**Closeness Centrality**	**Node**	**Closeness Centrality**
Trust	0.271	ESRC	0.157
NHS	0.242	NCSC	0.155
Digital	0.239	Williams	0.154
The Hillingdon Hospitals NHS Foundation Trust	0.239	EPSRC	0.153
CQC	0.229	AI	0.152
RCA	0.229	Cyber Security	0.152
NHS Foundation Trust	0.227	Oxford	0.151
Board	0.225	Digital	0.150
Richard Sumray	0.224	University	0.150
Shane DeGaris	0.224	Morello	0.148
2021		2022	
Node	**Closeness Centrality**	**Node**	**Closeness Centrality**
State	0.189	NCSC	0.145
National Cyber Strategy	0.187	AI	0.145
UKRI	0.183	Cyber Security	0.144
Department	0.178	Google	0.143
NCF	0.178	NCA	0.141
NCSC	0.176	Computer Science	0.140
NATO	0.175	SGN	0.138
EU	0.175	Microsoft	0.137
Industrial Strategy	0.174	Quantum	0.137
DSbD	0.173	GCHQ	0.137
2023		2024	
Node	**Closeness Centrality**	**Node**	**Closeness Centrality**
Lancaster University	0.144	CHERI	0.170
NCSC	0.142	AI	0.166
Cyber Security	0.141	Morello	0.157
EPSRC	0.139	Google	0.157
Microsoft	0.139	NCSC	0.155
Thales	0.138	UKRI	0.155
AI	0.138	Digital Security	0.154
ARM	0.138	Microsoft	0.153
Amazon	0.136	Rust	0.152
BT	0.135	EDA	0.152

The growing prominence of cybersecurity and technological nodes is evident starting in 2020, with the "NCSC" becoming increasingly central (degree: 0.073 in 2021, closeness: 0.176). This reflects the rising importance of cybersecurity frameworks in response to global threats. By 2024, the network's focus transitions to advanced technologies, as highlighted by nodes such as "CHERI" (degree: 0.050, closeness: 0.170) and "Digital Security" (degree: 0.026, closeness: 0.154). By 2023, "AI" entered the network as a central player (red node in Figure 6e), reflecting the rapid adoption and integration of AI technologies into digital security strategies. The surge in AI centrality during 2024 (red node in Figure 6f) suggests that AI tools have become key components in tackling security challenges, such as threat detection, automated responses, and risk management. This sharp rise may be attributed to the increasing accessibility of AI technologies, growing trust in AI-driven solutions, and the widespread adoption of AI tools across various sectors. These entities represent cutting-edge advancements in AI, secure hardware architectures, and digital security, which have become critical to the network's structure.

Funding and research organisations, including "UKRI" and "EPSRC", maintain consistent relevance throughout the timeline, signifying their role in enabling technological and scientific progress. In 2020, funding bodies like "ESRC" also emerge as key nodes, indicating their influence during a transitional phase where investments in cybersecurity and digital transformation began to take centre stage. By 2024, industry players such as "Google" (closeness: 0.157) and "Microsoft" (closeness: 0.153) gain central positions in the network, underscoring the increasing influence of large technology corporations in driving advancements and shaping interactions within the system.

In general, this temporal analysis demonstrates the highly dynamic nature of DSbD, with a focus on the network constantly evolving in response to emerging threats, technological innovations, and policy changes. As new actors and technologies emerge, the DSbD landscape adapts, highlighting the critical interplay between regulatory bodies, research institutions, and industry leaders. The ability to track these changes over time provides a unique opportunity to anticipate future trends, identify potential vulnerabilities, and guide strategic investment in areas such as AI, hardware security, and regulatory frameworks. The evolving prominence of entities within the DSbD landscape illustrates that digital security is not a static field; rather, it is continuously shaped by external factors such as technological advancements, geopolitical shifts, and societal demands for greater security and privacy. This dynamic quality underscores the need for ongoing monitoring and adaptability in the development of DSbD strategies, ensuring that security solutions remain robust and responsive to the ever-changing digital environment.

As we look ahead to the future, the trends identified in the temporal analysis presented herein provide a foundation for making informed predictions about the future direction of DSbD. Based on the continued evolution of aforementioned relationships, technologies, and entities within this rapidly expanding field, there is an indication that:

1. AI's Continued Dominance: AI will remain at the forefront of DSbD. As AI tools continue to evolve and become more sophisticated, their role in automating security processes, improving threat detection, and mitigating risks will likely expand. AI's integration into both offensive and defensive cyber capabilities is expected to grow, leading to an increase in research and development focused on AI-driven security solutions. We also anticipate further advancements in explainable AI and trust frameworks that ensure AI's decisions are transparent and reliable.
2. Emergence of Quantum Computing as a Central Player: Given the current rapid developments in quantum computing, we expect quantum technologies to become a more prominent node in the DSbD landscape. With the potential for quantum computers to break current encryption methods, there will be significant attention on post-quantum cryptography and new hardware security mechanisms to safeguard data and communications. This may also prompt an increase in collaboration between research institutions, industry, and government bodies to develop quantum-resistant solutions.

3. Strengthening of Regulatory and Compliance Frameworks: In 2025, the role of regulatory bodies like the EU and national cybersecurity agencies such as "NCSC" will continue to grow as new policies and guidelines are introduced to govern AI, quantum technologies, and digital security innovations. We anticipate an increased focus on global standards and cross-border collaborations to ensure the secure deployment of these emerging technologies.
4. Growth of Secure Hardware Solutions: The prominence of "CHERI" in 2024 suggests that secure hardware will remain a critical area of focus. In 2025, we predict more widespread deployment of hardware-based security solutions, particularly in critical infrastructure sectors such as defence, finance, and healthcare. Innovations like Morello and other hardware security projects will likely see increased adoption as organisations look for robust defences against sophisticated cyber threats that target hardware vulnerabilities.
5. Greater Collaboration Amongst Diverse Stakeholders: As the DSbD network grows more complex, we anticipate increased collaboration among government agencies, industry leaders, academia, and international bodies. This will be necessary to address the multifaceted challenges posed by emerging technologies, such as AI, quantum computing, and secure hardware. Research funding from bodies like "UKRI" and "EPSRC" will continue to play a pivotal role in fostering interdisciplinary approaches and innovative solutions.
6. Rise of New Ethical and Privacy Concerns: As digital security technologies advance, ethical and privacy concerns are expected to take centre stage in 2025. The increased use of AI, combined with the growing adoption of surveillance technologies and biometric security measures, will spark debates on user rights, data privacy, and the ethical use of technology. Trust frameworks will need to evolve to ensure that security solutions remain aligned with societal values and legal requirements.

5. Conclusions

This paper presents an exploration of the evolution of Digital Security by Design (DSbD) using a comprehensive data-driven approach, focusing on extracting key entities and relationships from textual documents published between 2019 and 2024. By extracting key entities and visualising their relationships using network analysis, the complex landscape of organisations, individuals, and interactions that have played a significant role in shaping DSbD over the years was mapped. The resulting networks allowed the identification of shifts in focus over time, such as the growing prominence and influence of AI technologies, secure hardware initiatives such as CHERI, and the foundational role of trust in digital security frameworks.

The temporal analysis revealed the significant growth and dynamic nature of the DSbD ecosystem, with the rapid expansion of relationships and collaborations, particularly in recent years. Key findings include the growing centrality of "Trust" and "AI" in network discussions, reflecting their pivotal roles in shaping security strategies. The dynamic prominence of entities such as "UKRI", "EPSRC", and "NCSC" highlighted the critical contributions of research funding bodies and national security organisations, while the centrality of "EU" underscored the impact of European regulatory influence. The introduction of hardware innovations like CHERI and the surge in AI-related discussions from 2023 onward marked key turning points in the DSbD landscape. These findings demonstrate the value of scalable text mining techniques and network analysis in uncovering hidden relationships and trends, providing actionable and valuable insights into the evolving nature of digital security and its key drivers, as well as prompting discussion of how such information can support making informed predictions about the future direction of DSbD.

This research not only enhances our understanding of how DSbD has developed but also offers a framework for future studies to monitor ongoing trends and anticipate future shifts in the landscape. The application of scalable text mining techniques and network analysis can continue to uncover relationships between entities, providing a foundation for identifying potential vulnerabilities and fostering collaboration between stakeholders. As digital security challenges evolve, the ability to track and understand these networks will be crucial in developing robust, adaptive, and forward-looking security strategies.

6. Future Directions

Given the positive findings of this initial study, several promising avenues can be explored to further enhance the understanding and practical impact of the DSbD landscape. One important direction is the expansion of ontological analysis, focusing on specific subdomains such as AI ethics, quantum-resistant cryptography, and hardware-based security. Delving deeper into these areas could provide new insights into how they interact within the broader DSbD framework. Additionally, as discussed in Section 4 building on the temporal analysis, future research could incorporate predictive modelling techniques to forecast trends and relationships within the DSbD network beyond 2025. Machine learning approaches could help anticipate shifts in the digital security landscape, offering valuable strategic guidance for industry, policy-makers, and researchers.

In future work, we plan to enhance our data processing pipeline through several strategies. To enhance preprocessing, we aim to apply NLP techniques such as tokenisation and lemmatisation alongside the NER applied in this study, with potential room to investigate robust duplicate detection and noise filtering methods like TF-IDF and outlier detection algorithms. Building upon the baseline established using co-occurrence methods, there is room to also integrate richer linguistic information through dependency parsing and contextual embeddings, which preliminary investigations suggest can significantly improve performance. Additionally, we plan to explore semantic role labelling to achieve more accurate and robust relationship extraction. By incorporating these advanced techniques and extending our data sources—integrating diverse datasets from global repositories, industry reports, and emerging digital security frameworks—we aim to build a more comprehensive, reliable, and meaningful dataset that forms a stronger foundation for future analyses.

Another potential area for future work is cross-sector analysis, exploring how DSbD principles are adopted and adapted across various sectors like healthcare, finance, and defence. Such comparative studies could identify sector-specific challenges and best practices, leading to the development of tailored security strategies. Additionally, the integration of global policy changes into the analysis would provide a deeper understanding of how regulations, such as those governing AI, data privacy, and quantum security, shape digital security practices. Incorporating human-in-the-loop systems within DSbD frameworks could also be explored, focusing on how human behaviour and decision-making influence security outcomes. This approach would enable the creation of more user-centric security solutions that balance technical robustness with usability.

Moreover, future work could investigate the ethical, social, and privacy implications of DSbD, particularly as they relate to AI, biometric security, and increased surveillance. Understanding the societal impact of these technologies is crucial for developing responsible and equitable digital security solutions. Another exciting area for exploration is the real-time adaptability of DSbD frameworks. By incorporating streaming data and continuously updating the ontology, researchers could enable faster detection of emerging trends and threats, providing stakeholders with actionable insights in near real time. These future research directions offer valuable opportunities to deepen the understanding of DSbD and address emerging challenges in this evolving field.

Author Contributions: Conceptualisation, methodology, validation, writing—original draft preparation, and writing—review and editing, H.K. and L.W.; funding acquisition, P.B. All authors have read and agreed to the published version of the manuscript.

Funding: For the purpose of open access, the author has applied a CC BY public copyright licence (where permitted by UKRI, 'Open Government Licence' or 'CC BY-ND public copyright licence' may be stated instead) to any Author Accepted Manuscript version arising. This work was funded by the Economic and Social Research Council (ESRC), grant 'Discribe—Digital Security by Design (DSbD) Programme'. REF ES/V003666/1.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The dataset collated as well as the scripting produced for the paper is available on GitHub (https://github.com/echokhan/Temporal-Network-Analysis-of-the-Evolution-of-Digital-Security-by-Design.git (accessed on 9 October 2024)).

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

References

1. Boot, A.W.; Thakor, A.V. Security design. *J. Financ.* **1993**, *48*, 1349–1378. [CrossRef]
2. Saltzer, J.H.; Schroeder, M.D. The protection of information in computer systems. *Proc. IEEE* **1975**, *63*, 1278–1308. [CrossRef]
3. Microsoft. *The Security Development Lifecycle*; Microsoft Press: Redmond, WA, USA, 2006.
4. Digital Security by Design. 2024. Available online: https://www.dsbd.tech/ (accessed on 18 October 2024).
5. Department for Digital, Culture, Media, and Sport. Digital Security by Design: Overview of Programme and Projects. 2021. Available online: https://www.nao.org.uk/wp-content/uploads/2023/03/dcms-departmental-overview.pdf (accessed on 18 October 2024).
6. Arm Limited. Digital Security by Design (DSbD): Transforming Digital Infrastructure Security Through Secure Hardware. 2020. Available online: https://www.arm.com/ (accessed on 18 October 2024).
7. Shrobe, H.; Laddaga, R.; Balzer, R. Awareness: The building blocks of security. *IEEE Secur. Priv.* **2009**, *7*, 74–77.
8. Bhattacharya, S.; Kaabouch, N. A survey on security and privacy issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2011**, *15*, 1–24.
9. Sarker, I.H.; Furhad, M.H.; Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *J. Big Data* **2021**, *8*, 1–29. [CrossRef]
10. UK Research and Innovation (UKRI). 2024. Available online: https://www.ukri.org/ (accessed on 1 November 2024).
11. The National Cyber Security Centre (NCSC). 2024. Available online: https://www.ncsc.gov.uk/ (accessed on 1 November 2024).
12. Watson, R.; Moore, S.; Sewell, P.; Davis, B.; Neumann, P. Capability Hardware Enhanced RISC Instructions (CHERI). 2024. Available online: https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/ (accessed on 18 October 2024).
13. Wang, Z.; Hu, Y. Towards a High-performance and Secure Memory System and Architecture for Emerging Applications. *arXiv* **2022**, arXiv:2205.04002.
14. He, Z.; Elizarov, M.S.; Li, N.; Xiang, F.; Fratalocchi, A. Quantum-activated neural reservoirs on-chip open up large hardware security models for resilient authentication. *arXiv* **2024**, arXiv:2403.14188.
15. Malatji, M.; Tolah, A. Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. *AI Ethics* **2024**, 1–28. [CrossRef]
16. Hashmi, E.; Yamin, M.M.; Yayilgan, S.Y. Securing tomorrow: A comprehensive survey on the synergy of Artificial Intelligence and information security. *AI Ethics* **2024**, 1–19. [CrossRef]
17. Sarker, I.H. Introduction to AI-Driven Cybersecurity and Threat Intelligence. In *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 3–19.
18. de Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics* **2023**, *12* 1920. [CrossRef]
19. Wahyuningsih, T.; Sembiring, I.; Setiawan, A.; Setyawan, I. Exploring network security threats through text mining techniques: A comprehensive analysis. *Comput. Sci. Inf. Technol.* **2023**, *4*, 258–267. [CrossRef]
20. Mukhopadhyay, A.; Sharma, K. A Text-Mining Approach to Cyberrisk Management. 2021. Available online: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/a-text-mining-approach-to-cyberrisk-management (accessed on 18 October 2024).

21. Ignaczak, L.; Goldschmidt, G.; Costa, C.A.D.; Righi, R.D.R. Text mining in cybersecurity: A systematic literature review. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
22. Barik, K.; Misra, S.; Konar, K.; Kaushik, M.; Ahuja, R. A comparative study on the application of text mining in cybersecurity. *Recent Adv. Comput. Sci. Commun. (Formerly Recent Patents Comput. Sci.* **2023**, *16*, 80–93. [CrossRef]
23. Radanliev, P. Digital security by Design. *Secur. J.* **2024**, 37, 1640–1679. [CrossRef]
24. Saqr, M. Temporal Network Analysis: Introduction, Methods and Analysis with R. In *Learning Analytics Methods and Tutorials: A Practical Guide Using R*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 541–567.
25. Gelardi, V.; Le Bail, D.; Barrat, A.; Claidiere, N. From temporal network data to the dynamics of social relationships. *Proc. R. Soc. B* **2021**, *288*, 20211164. [CrossRef] [PubMed]
26. Mishra, M.; Vishwakarma, S.K.; Malviya, L.; Anjana, S. Temporal analysis of computational economics: A topic modeling approach. *Int. J. Data Sci. Anal.* **2024**, 1–15. [CrossRef]
27. Huang, L.; Chen, X.; Zhang, Y.; Wang, C.; Cao, X.; Liu, J. Identification of topic evolution: Network analytics with piecewise linear representation and word embedding. *Scientometrics* **2022**, *127*, 5353–5383. [CrossRef]
28. Zhang, D.C.; Lauw, H. Dynamic topic models for temporal document networks. In Proceedings of the International Conference on Machine Learning, Baltimore, MD, USA, 17–23 July 2022; pp. 26281–26292.
29. Jing, X.; Hu, Q.; Zhang, Y.; Rayz, J.T. Tracing topic transitions with temporal graph clusters. *arXiv* **2021**, arXiv:2104.07836. [CrossRef]
30. Scrapy. 2024. Available online: https://scrapy.org (accessed on 18 October 2024).
31. Pandas. 2024. Available online: https://pandas.pydata.org/ (accessed on 8 October 2024).
32. SpaCy. 2024. Available online: https://spacy.io/ (accessed on 18 October 2024).
33. Zhong, Z.; Chen, D. A frustratingly easy approach for entity and relation extraction. *arXiv* **2020**, arXiv:2010.12812.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.