Decoding CyberSecurity: How Terminology Shapes the Field

BERTHOLAT Jean

UMR LAMSADE, Dauphine University PSL, France; Innovation Department, Alten SA, France. E-mail: jean.bertholat@atlen.com*

MERAD Myriam

UMR LAMSADE, Dauphine University PSL, France. E-mail: myriam.merad@lamsade.dauphine.fr*

Cybersecurity stands at the forefront of protecting today's digital infrastructures and personal data. While significant technical and organizational advances have been made, it is crucial to periodically step back and question whether our current cybersecurity philosophy, concepts and models remain fit for purpose of resilience in a rapidly evolving environment. This collection of essays critically examines the prevailing understanding of cybersecurity, contrasts it with an alternative vision, and explores the foundational model on which this practice is based. Rather than offering a definitive new definition, the intention is to "shake things up" and provoke a deeper conversation on whether a shift in paradigm is warranted. By challenging the assumptions held by researchers, practitioners, and policymakers, this work aims to foster innovative thinking that can guide cybersecurity toward a more resilient and adaptive future model. Ultimately, it is a call to reassess current approaches and inspire further debate, research, and action, ensuring that our strategies remain aligned with the emerging challenges of a never-ending increase interconnected digital world. This article serves as an initial exploration into the meaning of the term "*cyber()security*", analysing how its usage and interpretation evolve, shaped by the communities of practice that have adopted it.

Keywords: essay, cybersecurity, cyber security, concept, definition, theories, model, risk

1. Introduction

"It's a future job," "we really need it today!"; these are the sentences often uttered when one mentions working in cybersecurity. But, if you work in the field yourself, would you be able to clearly explain, in just a few words, what cybersecurity truly entails and why it should matter to those who may not fully understand why they are expressing such statements?

The adoption of cybersecurity measures in organizations today is largely driven by fear of regulatory or normative sanctions, financial losses, and other adverse consequences (IBM 'Cost of a Data Breach' 2024). It is well documented that many organizations only allocate significant resources to cybersecurity after experiencing a first incident[a]. This reactive behaviour can be attributed in part to cognitive biases such as optimism bias—where individuals believe "it won't happen to me"—and a general tendency to underestimate risks until a concrete alert occurs. Behavioural studies (Kahneman and Tversky 1979) further illustrate that recent or emotionally significant events disproportionately influence security investment decisions—a pattern not unique to cybersecurity but observable across various domains where prevention is undervalued until a crisis strikes.

Thus, investing intelligently in cybersecurity is the optimal strategy to ensure rapid recovery of normal operations. This approach avoids the significantly higher, often uncalculated expenditures incurred reactively after a breach, ultimately proving both more cost-effective and efficient in minimizing downtime of operations.

That is the "what", that we are all aware of, but talking about the" how" is where scientific backgrounds and politics start to struggle. When considering the "how," the

[a] In cybersecurity, incident refers to an event without implying severity, unlike in risk management, where events are classified by severity from incident to catastrophe.

Proceedings of the 35th European Safety and Reliability and the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage & Marja Ylönen
Copyright © 2025 by ESREL2025 & SRA-E 2025 Organizers. Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2022-paper

discussion frequently turns toward technical solutions. However, this essay deliberately diverts from an exclusive focus on technological implementations, instead examining the governance dimension and the critical **research question of how to motivate decision-makers to integrate security considerations into their overall strategic frameworks.**

In this essay, we will explore two main lines of thought. First, we will examine the motivation behind the effort to find solutions that could further democratize and broaden the adoption of cybersecurity approach among decision-makers. Next, we will focus on a hypothesis and the barriers that hinder greater engagement in this process. This will involve exploring how the proposed hypothesis could be practically implemented to enhance cybersecurity adoption.

2. Current Landscape and Motivations

Although there is a current trend, particularly evident in large private organizations, toward incorporating cybersecurity into strategic planning, the effectiveness of cyber policies appears strongly correlated with the financial resources available. In essence, the greater the monetary commitment, the more likely it is that the full spectrum of cybersecurity needs is addressed for an organization; yet, this financial capability may also lead organizations to invest in areas that are not necessarily relevant to enhance cybersecurity posture.

In contrast, smaller organizations or those with limited resources, public entities, or industries with distinct cultural approaches lack the capacity to invest in superfluous cybersecurity measures. They require a more intelligent and refined approach that optimizes the balance between investment and the effectiveness of security controls, as they cannot afford measures that do not directly address their specific risk profiles, unlike larger organizations with greater financial flexibility.

Even with no consistent multi-year studies found, analysis of cybersecurity yearly reports[b], the number of organizations that seriously plan or invest on cybersecurity seems to have reached a ceiling in recent years (Observe ‘The State of Observability' 2023). This observation suggests that, despite growing communication around cyber threats, many organizations have yet to translate this information into a sustained commitment to comprehensive cybersecurity strategies. Consequently, the main **cybersecurity adoption driver: Fear of incident**, does not provide sufficient incentive for a wide range of organizations to proactively invest in robust cybersecurity plans.

2.1.*Hypothesis for adoption and barriers*

Thus, let ask ourselves what else could motivate cybersecurity adoption. **Does a clear and comprehensive explanation of what cybersecurity truly encompasses could serve as a missing catalyst?** This clarity could motivate the latest organizations whose cyber protection strategy is currently inadequate, and who lack a resilient cyber interconnection system, to integrate cybersecurity more effectively into their core operational strategies.

However, understanding the philosophy of cybersecurity today demands significant personal investment from non-experts. This deep engagement is essential for crafting a cybersecurity strategy that is truly aligned with an organization’s value creation objectives, rather than relying on generic solutions offered by consultants who, despite commanding high fees, often deliver the same strategy recommendations across different clients (Villesalmon 2016).

Cybersecurity is an interdisciplinary practice applicable to a vast majority of activities in today’s interconnected world. However, this “I cut across all domains” and “non-specialized” aspect often leads non-experts to perceive the field as nebulous, vague, and impenetrable. This intangible and somewhat disorganized image, considered as an exclusive domain of a few hand-picked specialists, preventing both

[b] Regarding: CSIRP usage (Ponemon Institute’s Cyber Resilient Organization Report 2015 & 2020), Nb employees devoted to cybersecurity (ISACA State of Cybersecurity 2020–2024), self-declared resilient organizations (WEF Global Cybersecurity Outlook 2025).

development and, more importantly, the widespread adoption of cybersecurity across our society. Although the practice has existed for several decades, it is only recently that efforts have been made to explain it in simple, accessible terms to all, as illustrated by initiatives such as (‘DemainSpécialisteCyber’ 2023).

On the other hand, effective cybersecurity must be tailored to the specific needs and characteristics of each organization. Consequently, individuals with a detailed and comprehensive vision of organization’s objectives and specificities should lead the orchestration of cybersecurity within their systems. Thus, this responsibility falls to organizational leaders such as board members, CTOs, CEOs, as well as government officials like ministers and heads of state, essentially anyone tasked with formulating strategies to achieve clearly defined goals. To some extent, this aligns with the recommendations of various established frameworks, such as ISO 27001, which emphasizes the involvement of leadership as a primary recommendation.

Unfortunately, regulations don’t make those individuals engaging with cybersecurity for the right reasons, which makes them even less inclined to develop an efficient understanding of the practice. In our view, it is precisely these non-experts who must be persuaded to take a real interest in cybersecurity, ensuring that the resilience of the **interconnection systems** upon which their global activities rely is optimized. Even more that research has demonstrated that the adoption of cybersecurity technologies has a beneficial impact on organizational performance (Hasani et al. 2023).

On another note, although we won't delve into this topic in detail here, it’s equally important to engage the younger generation who will eventually be responsible for enhancing cybersecurity. The field is already suffering with a shortage of skilled professionals, and it's not getting any better for the future (Observe ‘The State of Observability' 2023). Furthermore, the influx of capital driven by emerging technologies like artificial intelligence, fuelled by the recent surge in genAI, will only intensify the competition for new talent. Unlike clearly defined careers such as firefighting, law enforcement, or medicine, cybersecurity is not as straightforward, making it harder for young people to picture themselves in such roles. This challenge is illustrated by the fact that many young people aspiring to work in cybersecurity only see themselves as pentesters, having identified at some point with black, grey hat hackers. These perceptions underscore the urgent need to formalize, clarify and distribute the cybersecurity philosophy, a goal that initiatives like (‘DemainSpécialisteCyber’ 2023.) have already begun to address, and this article aims to contribute to that effort.

3. Defining Cybersecurity: A Question That Keeps Resurfacing

"What the f*ck is cybersecurity?", a question that has been asked by an exponentially growing number of people since 2010, Fig.1

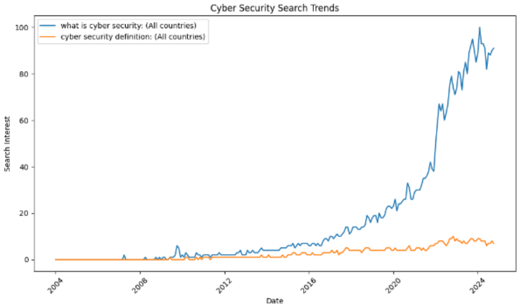

Fig.1 'What is cyber security search' - GoogleTrends

The increasing omnipresence of digital technologies has made cybersecurity a central concern, yet its precise definition and scope remain elusive for many.

This question resonates across a broad spectrum of individuals. If you are a child experimenting beyond the conventional boundaries of digital technologies and have heard that such exploration could one day become a career, you might ask it. If you are a student navigating future career prospects and trying to understand where cybersecurity fits in, you might ask it. If you have spent some years in the field but still wonder how cybersecurity approach is structured, you might ask it. Even if you have a well-formed vision of cybersecurity but seek to challenge and refine your perspective, this question may still cross your mind.

In all these scenarios, and for countless other reasons, the underlying need remains the same: a deeper understanding of the fundamental principles and inner workings of cybersecurity that extend beyond technical aspects to encompass its strategic, organizational, and human dimensions. This recurring question: "What the f*ck is cybersecurity?", is not simply rhetorical; it reflects a broader challenge in defining, structuring, and communicating the essence of this field.

3.1.*No simple answer*

To begin, it is essential to acknowledge that this question does not have a straightforward answer that can be condensed into a few lines, nor will it necessarily have a universally accepted definition in the future. Defining a concept that is **inherently intertwined with a multitude of other disciplines** is far more complex than defining a tangible concept with a clear function and well-established boundaries such as border security, which is defined by geographical limits and aims to control and regulate the movement of people and goods.

Even the analysis presented in this essay, built upon our own study and understanding of cybersecurity field, will likely be subject to debate. Some may challenge the perspective we offer, while others may find it aligns with their own views (which we hope will be the case for some). This essay is, above all, an invitation to reflect on the approach of cybersecurity rather than a definitive answer to what it is. It aims to provide food for thought, allowing readers to form their own perspective on the field.

we will try hard for clarity in our analysis to ensure that every argument presented can be challenged. As a starting point, we approached our search for understanding as anyone would when encountering an unfamiliar word: by examining how the term is constructed and exploring its definition – well, its various definitions. Although nearly everyone has heard of "cybersecurity”, forming a clear and comprehensive understanding of it remains challenging. Even experts in specific cyber subdomains may struggle to define it in a broader sense if they have never explicitly reflected on the field as a whole. Let's begin by analyzing the origins of the term “cybersecurity” and how it has been used over the years and across different contexts.

3.2.*In the beginning was “Creeper” (1971)*

While sources differ on the precise origins of the term "cyber" in its contemporary sense, there is broad consensus that the concept of cybersecurity emerged as a response to the growing need for protection surrounding the use of new exchange technologies. The appearance of the Creeper worm on the ARPANET network in 1971 may have been one of the earliest indicators of this awareness, highlighting the vulnerabilities inherent in interconnected systems. However, rather than delving into the exact etymology of the term, it is more relevant to examine how the term has evolved over time, shaped by shifting technological landscapes and security imperatives.

3.2.1.*Term evolution analysis methodology*

While the focus on scientific literature provided a structured and comprehensive dataset, the integration of media discourse and regulatory texts offers insights into societal and policy-driven interpretations of the term. Future studies could refine this analysis by including cross-linguistic comparisons, as terminology adoption often varies significantly between cultural and linguistic contexts.

For this purpose, we conducted an extensive review of research publications indexed in the Scopus database, which offers broader historical coverage than Web of Science (WoS). Our dataset consisted of 51,711 documents spanning from 1980 to 2025, explicitly referencing either cybersecurity or cybersecurity in titles, abstracts, or author keywords. The search query used was:

(TITLE-ABS (cyber **PRE/1** security) **OR** AUTHKEY (cyber **PRE/1** security)) **OR** (TITLE-ABS (cybersecurity) **OR** AUTHKEY (cybersecurity)).

Our analysis focused on key indicators such as term frequency, relative occurrence within the corpus, and co-occurrence trends.

Additionally, we leveraged VOSviewer (van Eck and Waltman 2007) to generate visual mappings, allowing for a more precise understanding of the contexts in which these terms have been used over time.

3.2.2.*Inconsistency in cybersecurity*

One of the first aspects that caught our attention when analysing cybersecurity was the inconsistency in terminology. Variants such as “cyber security”, “cybersecurity”, “cyber-security”, and even broader terms like “information security” and “IT security” are frequently used interchangeably, particularly by non-experts, despite the absence of a strict consensus. Creating another layer of complexity in an already intricate field.

This observation raises important questions about how terminology shapes meaning. The spelling and formulation of a term often influence its interpretation, which can vary across time periods, cultural contexts, and professional domains. A single word may carry different meanings depending on its usage; much like the term “bark”, which in everyday language refers to a dog's vocalization, while in botany, it denotes the outer layer of a tree.

Thus, the inconsistency in the terminology of "cybersecurity" extends beyond simple spelling variations; it reflects deeper divergences in how the field is conceptualized and communicated. Practitioners may adopt different terms based on their specific domain, while non-experts often relay terminology they have encountered without necessarily understanding its nuances. For example, organizations prioritizing “IT security” terminology often focus on confidentiality and technical solutions, while those adopting broader “cybersecurity” frameworks may incorporate governance and societal resilience into their models. This divergence has practical consequences: a narrow interpretation can lead to overlooked vulnerabilities in human and organizational systems, while a broader view may result in resource misallocation. Understanding these terminological impacts helps align strategic decisions with real-world risks.

We will explore the reasons behind this divergence later, but to illustrate this phenomenon, Fig.2 presents the evolution of the frequency of occurrence of the terms “cyber security” and “cybersecurity” in The New York Times Magazine over the years (Courson and Azoulay 2021).

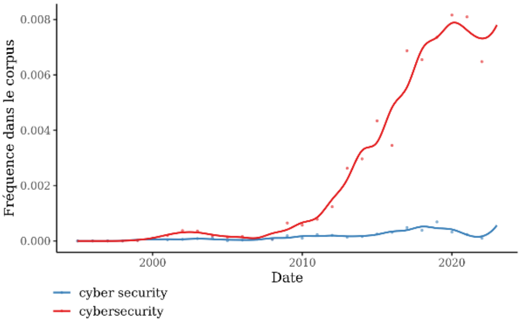

Fig.2 Evolution of the usage frequency of ‘cyber security’ and ‘cybersecurity’ in The New York Times Magazine over time

The trends observed in these curves clearly indicate that “cybersecurity” has become the dominant and, in practice, the sole term used by journalists when addressing cybersecurity topics for the general public.

So, beyond spelling differences, variations in terminology also reflect differences in meaning. Some sources use cybersecurity synonymously with “information security” or “IT security”, while others establish clear distinctions between these concepts. (Von Solms and Van Niekerk 2013) illustrate this divergence by arguing that cybersecurity extends beyond the protection of information and infrastructure; it also encompasses the security of all entities operating within cyberspace, shielding them from various forms of harm. we would add that this harm is not solely the result of malicious intent but can also arise from accidental failures or unintended consequences.

3.2.3.Chronological Evolution

While the media usage of “cybersecurity” appears consistent and unambiguous, can the same be said for its use in other contexts? The answer is no.

In the scientific domain, prior to 2003, the term “cyber security” was predominantly used, Fig.3. Furthermore, analyzing keyword cooccurrences from research published between 1980 and 2004 reveals that, after filtering out terms related to specific methods or activities within cybersecurity, the term “cyber security” was primarily associated with fields where security already had a strong presence. These included critical infrastructure (CI), homeland security, information security, and infrastructure protection. Furthermore, during this period, the military context remained closely linked to the term “computer security” (sample 1980-2004[c]).

Researchers initially focused on the security of national infrastructure, recognizing the emerging threats posed by the increasing reliance on digital interconnection technologies.

Extending the analysis by four to five additional years highlights a shift in terminology, where the rise of “cybersecurity” corresponds with a decline in the usage of “computer security”. Despite its decreasing occurrence, “computer security” appears to cede its position to “cybersecurity”, as both remain closely associated with military contexts such as “war” and “military”. This period also marks the emergence of connections between cybersecurity and regulatory frameworks, as well as the development of security standards (“European”, “iec 61850”).

At the same time, “cyber security” strengthens its association with homeland security and the protection of industrial infrastructure. This shift reflects growing concerns over digital threats targeting national territories, as exemplified by the increasing presence of terrorism-related discourse (sample 1980–2008).

As the years progress, the contextual usage of “cybersecurity” and “cyber security” becomes increasingly intertwined. However, both terms continue to retain some of their original distinctions. “Cybersecurity” remains primarily associated with governance, policy, awareness, strategy, education, and the broader concept of cyber defence. In contrast, “cyber security” maintains its connection to industrial contexts, such as industrial control systems (ICS) and smart grids, as well as early cyberattacks and operational defence techniques for intrusion and anomaly detection. Despite these distinctions, the overall discourse gradually converges toward a more unified terminology (sample: 1980–2016).

Today, a third major domain has emerged related to the field of cybersecurity: Machine learning (Bertholat and Merad 2025) is becoming increasingly prominent in cybersecurity discussions, further driving the convergence of the terminology’s “cybersecurity” and “cyber security”, as it is more frequently associated with the cybersecurity terminology. While both terms continue to be linked to similar topics, certain domains that could have traditionally been associated with “cyber security” terminology, such as Industry 4.0 and the Internet of Things (IoT), have now shifted toward the realm of cybersecurity. As this distinction continues to fade, “cybersecurity” appears to be gaining dominance within scientific discourse, Fig.3.

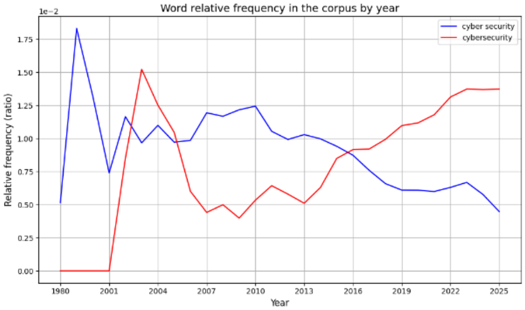

Fig.3 Word relative frequency in the corpus by year

Assessing the evolution of terminology in regulations and standards is more challenging, but it appears to follow the broader trend. For instance, the NIST, in its communications prior to 2008, predominantly used the two-word term “cyber security”, whereas in more recent publications, the shift toward the one-word form “cybersecurity” has become evident.

In common usage, both terms have followed a similar trajectory, with “cyber security” initially gaining traction slightly earlier. However, the gap between them has gradually narrowed, further reinforcing the notion that “cybersecurity” is becoming increasingly dominant across all domains Fig.4.

[c] GitHub

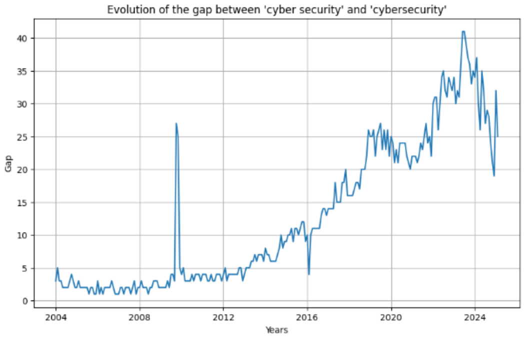

Fig.4 Gap evolution between 'cyber security' and 'cybersecurity' – GoogleTrends

3.3.*Cybersecurity terminology conclusions*

This analysis highlights the evolving usage of "cyber security" and "cybersecurity", reflecting shifts in context, focus, and audience over time. Initially, "cyber security" was predominantly associated with industry and homeland security, while computer security remained closely tied to military and warfare-related concerns. Over time, as cyberthreats and cybercrime gained prominence in political and strategic discussions, the term "cybersecurity" gradually replaced "computer security" in these contexts, with a noticeable peak in usage around 2003–2004 likely influenced by heightened media coverage of major cyberattacks such as Blaster, SoBig, and MyDoom.A.

Today, the distinction between the two terms persists, though their boundaries continue to blur. "Cyber security" remains the preferred terminology among technical professionals, particularly in operational and industrial settings. Meanwhile, "cybersecurity" has become the dominant term in broader discourse, extending beyond policy and governance to encompass emerging technologies such as the Internet of Things (IoT), blockchain, and machine learning.

This trend suggests a gradual standardization of terminology, with "cybersecurity" increasingly asserting itself as the prevailing term across multiple domains.

If we consider the initial perspective, as scientists, we originally discussed the security of a specific object. However, over time, the term has expanded in scope, evolving beyond both the notion of cyber and the concept of security to become a broader, more encompassing idea.

Therefore, in our future work we will use the one-word term "cybersecurity". It will be used to represent this concept, not simply as the pursuit of a secure state for cyber related systems but as a reflection of the growing need for a multidisciplinary, collaborative approach. This shift acknowledges that achieving resilience in our interconnected systems requires more than just isolated security measures; it demands a holistic framework that integrates technological, strategic, and policy-driven efforts.

4. Future Works

In the previous section, we took a position on the evolution of terminology, though our focus remained primarily on the scientific domain, with some consideration given to media discourse and a more succinct analysis of other contexts. While this study provides valuable insights, a more extensive exploration of these aspects could be conducted through specialized research in discourse analysis. Although certain simplifications have been made, this analysis still offers a meaningful perspective on the subject and highlights its significance.

Future research could expand upon this work by conducting more in-depth analyses across additional corpuses, examining how the terminology is used over time in regulatory, industrial, and public discourse. Furthermore, a systematic study of definitions across various sources could offer deeper insights into the evolving meaning of cybersecurity. Working with well defined dataset like the one provided by European data initiative for regulatory studies.

While understanding terminology provides valuable insights into how cybersecurity is framed, it remains insufficient to determine whether clearer explanations alone could drive decision-makers toward stronger cybersecurity adoption. Addressing this question requires a broader investigation beyond linguistic distinctions, focusing on the definitions and practical models that shape cybersecurity as a discipline nowadays. Expanding this analysis will help clarify how different fields conceptualize the term and its implications, ultimately contributing to a more structured and accessible understanding of cybersecurity.

Reducing ambiguity in its definition may also help lower barriers to entry for newcomers and facilitate a more cohesive discourse across disciplines. In other words, future efforts should focus on the creation of a collaborative standardization framework. This could involve the development of a global cybersecurity lexicon, co-created by researchers, practitioners, and policymakers, to reduce terminological ambiguities. Such an initiative could build on existing standards like ISO 27001, ensuring that the language used across disciplines aligns with the practical needs of different stakeholders. This will be the focus of forthcoming PhD research.

Although our primary interest lies in securing the cyber ecosystem within industrial contexts ("cyber security"), we will align with the broader conceptual shift toward using the term cybersecurity to encompass activities within this overarching discipline.

This perspective aligns with our broader objective of developing and promoting a risk-based approach that engages the entire decision-making chain to enhance the cybersecurity resilience of interconnected infrastructures, rather than focusing solely on securing individual cyber assets.

5. Conclusion

In conclusion, the analysis of terminology is not a mere academic exercise; it profoundly shapes the way we approach, model, and solve problems within the field of cybersecurity. The evolution and usage of terms influence not only the comprehension of the domain but also the methodologies, models, and strategies deemed appropriate to address its challenges. As this study has shown, inconsistencies and shifts in terminology reflect broader conceptual changes that, in turn, impact the effectiveness and consistency of proposed solutions. Future research must continue to explore these dynamics, emphasizing the critical role of language in framing the priorities and decisions of both researchers and practitioners. By fostering a more structured and reflective approach to terminology, we can enhance the coherence and adaptability of cybersecurity solutions, ensuring they remain relevant in an increasingly interconnected world.

Now that we have explored the evolution and implications of cybersecurity terminology, we can return to the fundamental question posed at the beginning of this work: What is cybersecurity?

References

Bertholat, Jean, and Merad, Myriam. 2025. 'Practical Use of AI for Cyber Risk Management in Critical Infrastructures: A Review'. In , 33.

'Cost of a Data Breach 2024 | IBM'. n.d. Accessed 7 February 2025. https://www.ibm.com/reports/data-breach.

de Courson, Benoît, and Azoulay, Benjamin. 2021. 'Gallicagram : Un Outil de Lexicométrie Pour La Recherche'. OSF. https://doi.org/10.31235/osf.io/84bf3.

'DemainSpécialisteCyber'. n.d. Accessed 6 February 2025. https://www.demainspecialistecyber.fr/.

Van Eck, Nees Jan, and Waltman, Ludo. 2007. 'VOS: A New Method for Visualizing Similarities Between Objects'. In *Advances in Data Analysis*, edited by Reinhold Decker and Hans -J. Lenz, 299–306. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-70981-7_34.

Hasani, Tahereh, Norman O'Reilly, Ali Dehghantanha, Davar Rezania, and Nadège Levallet. 2023. 'Evaluating the Adoption of Cybersecurity and Its Influence on Organizational Performance'. *SN Business & Economics* 3 (5): 97. https://doi.org/10.1007/s43546-023-00477-6.

Kahneman, Daniel, and Amos, Tversky. 1979. 'Prospect Theory: An Analysis of Decision under Risk'. *Econometrica* 47 (2): 263–91. https://doi.org/10.2307/1914185.

Miller, Benjamin. 2001. 'The Concept of Security: Should It Be Redefined?' *Journal of Strategic Studies* 24 (2): 13–42. https://doi.org/10.1080/01402390108565553

'The Approach to Risk-Based Cybersecurity | McKinsey'. n.d. Accessed 10 December 2024. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity.

'The State of Observability 2023'. n.d. Observe, Inc. Accessed 9 February 2025. https://www.observeinc.com/resources/the-state-of-observability-2023/.

Villesalmon, Eric. 2016. 'Les travers de la cybersécurité - la méthode pour la méthode'. *ISLEAN* (blog). 10 November 2016. https://islean-consulting.fr/fr/organisation-dsi/les-travers-de-la-cybersecurite-la-methode-pour-la-methode/.

Von Solms, Rossouw, and Van Niekerk, Johan. 2013. 'From Information Security to Cyber Security'. *Computers & Security* 38 (October):97–102. https://doi.org/10.1016/j.cose.2013.04.004.