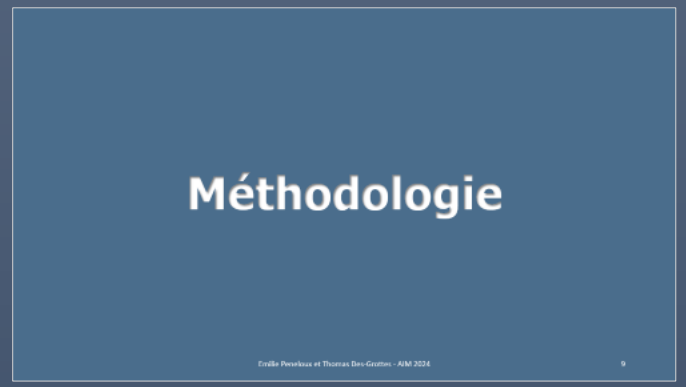
Risque cyber ou risque pour la sécurité de l'information ?

Entre prisme académique et prisme professionnel – une mise en perspective


Introduction
Emilie Peneloux et Thomas Des-Grottes - AIM 2024
3


Question de recherche
Emilie Peneloux et Thomas Des-Grottes - AIM 2024
7


Méthodologie
Emilie Peneloux et Thomas Des-Grottes - AIM 2024
9


Résultats
Emilie Peneloux et Thomas Des-Grottes - AIM 2024
13


Limites de cette recherche
Emilie Peneloux et Thomas Des-Grottes - AIM 2024
26

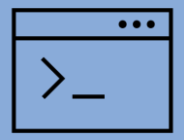

Recommandations pour de futures recherches

Introduction

Introduction

Hausse de 400% des cyberattaques en France depuis 2020.

L’impact financier moyen pour les PME est compris entre 300 000 et 500 000 euros.



Une atteinte à la cybersécurité se produit toutes les 39 secondes.

La faille humaine est la plus exploitée.

Développement de la cybersécurité

Risque de sécurité informatique

Risque de sécurité de l'information

Risque cyber (ou de cybersécurité)

Confusion sémantique que certains auteurs ont cherché à réduire (von Solms & van Niekerk, 2013 ; Alshaikh et al., 2014 ; Craigen et al., 2014 ; Finne, 2000 ; Schatz, Bashroush & Wall, 2017).

Les notions sont analogues (voir par exemple de Sagazan, 2020 ou Ögüt, 2011).

Les notions sont proches mais diffèrent dans leur périmètre (von Solms & van Niekerk, 2013).

Dans la littérature

Aucune définition globalement acceptée dans la littérature.

Strupczewski recense 20 définitions dans la littérature en 2021 et propose une définition interdisciplinaire :

« *Cyber-risk is an operational risk associated with performance of activitites in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber risk' also includes physical threats to the ICT resources within organisation* » (p.6).

Dans le monde professionnel

Le monde professionnel semble gêné par cette absence de définition.

Les normes et cadres ne semblent pas résulter d'une collaboration interdisciplinaire et internationale.

Cela peut conduire à un frein à une réponse robuste et résiliente face aux problématiques de cybersécurité (Chaudhary et al., 2018).

Question de recherche

Question de recherche

Le risque cyber et le risque pour la sécurité de l'information sont-ils analogues ?

La différence d'usage résulte-t-elle d'une appropriation académique vs opérationnelle ?

Puisque «l*a signification, c'est l'usage* » (Wittgenstein, 1961), nous nous demandons quelle terminologie est employée pour caractériser le risque de cybersécurité dans les milieux professionnel et académique et pour quel usage ?

Méthodologie

Revue académique

Une revue conceptuelle (Paré et al., 2023).

Chercher à affiner des concepts ambigus ou à clarifier des conceptions trop utilisées ou vagues (Paré et al., 2023).

Une analyse thématique Paillé & Mucchielli, 2016) .

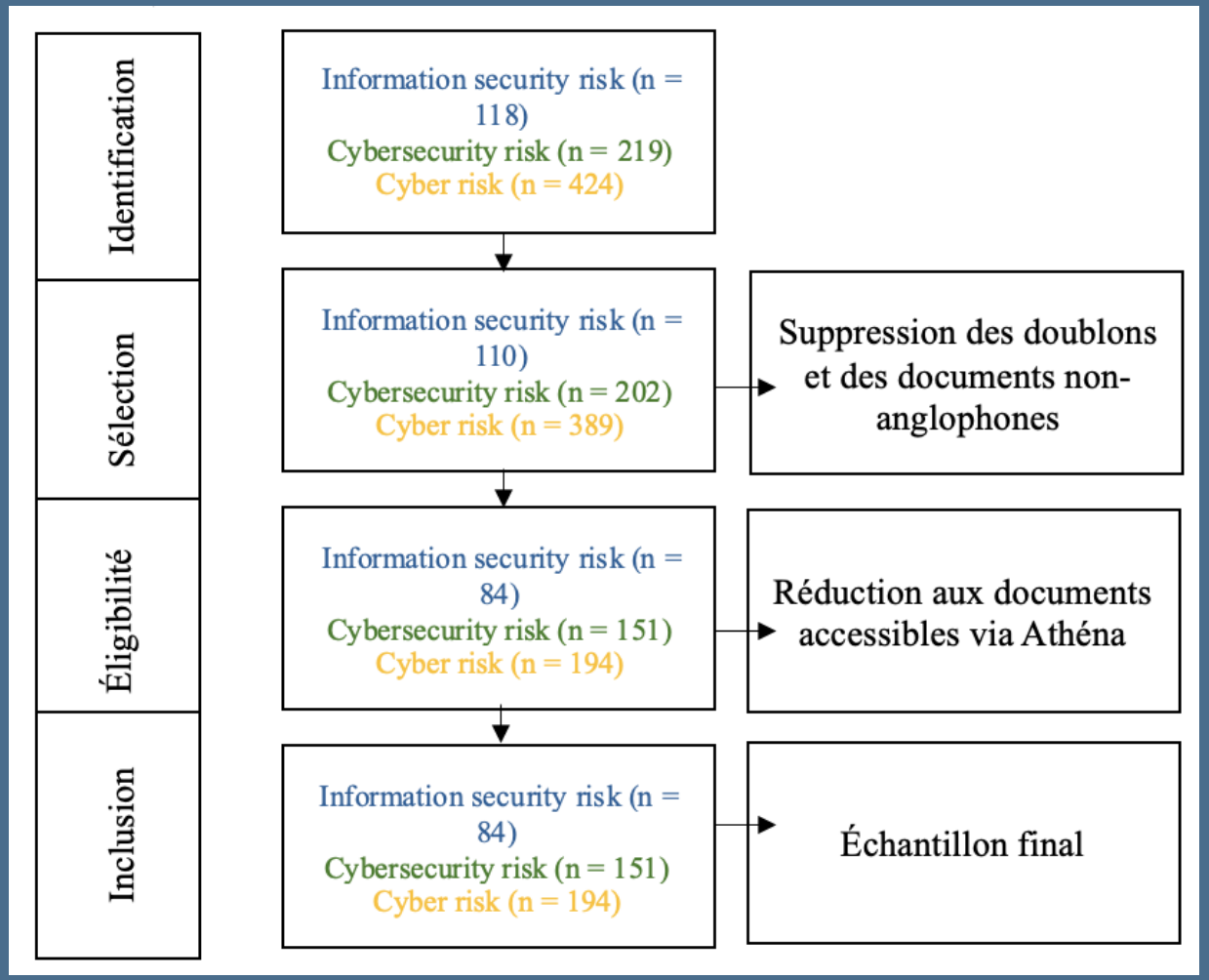
Revue professionnelle

Un examen de la portée (Paré et al., 2015).

Recensement d'un échantillon d'instances et de documents de l'écosystème cyber.

Recensement des termes utilisés et de leurs définitions associées.

Revue académique



Une revue conceptuelle (Paré et al., 2023).

Chercher à affiner des concepts ambigus ou à clarifier des conceptions trop utilisées ou vagues (Paré et al., 2023).

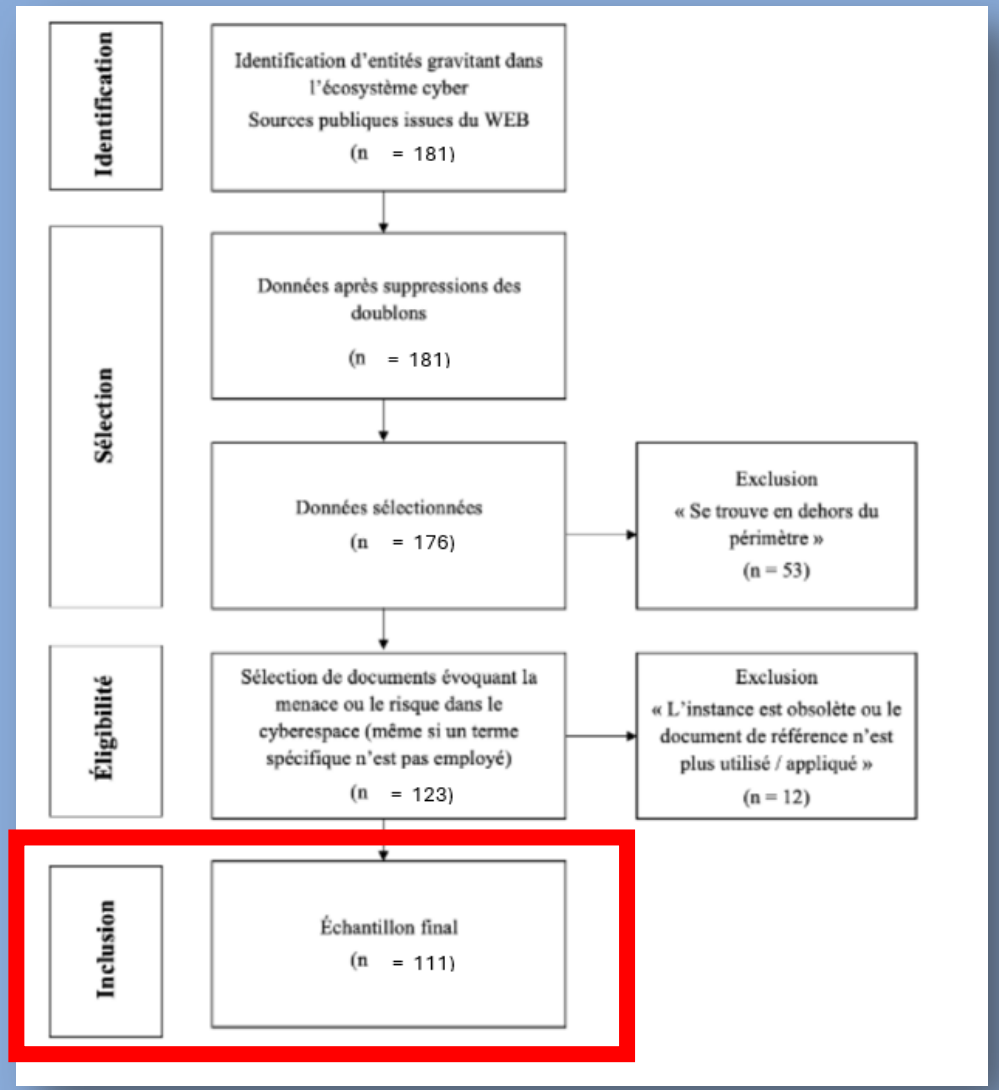
Une analyse thématique Paillé & Mucchielli, 2016) .

Revue professionnelle

Un examen de la portée (Paré et al., 2015).

Recensement d'un échantillon d'instances et de documents de l'écosystème cyber.

Recensement des termes utilisés et de leurs définitions associées.



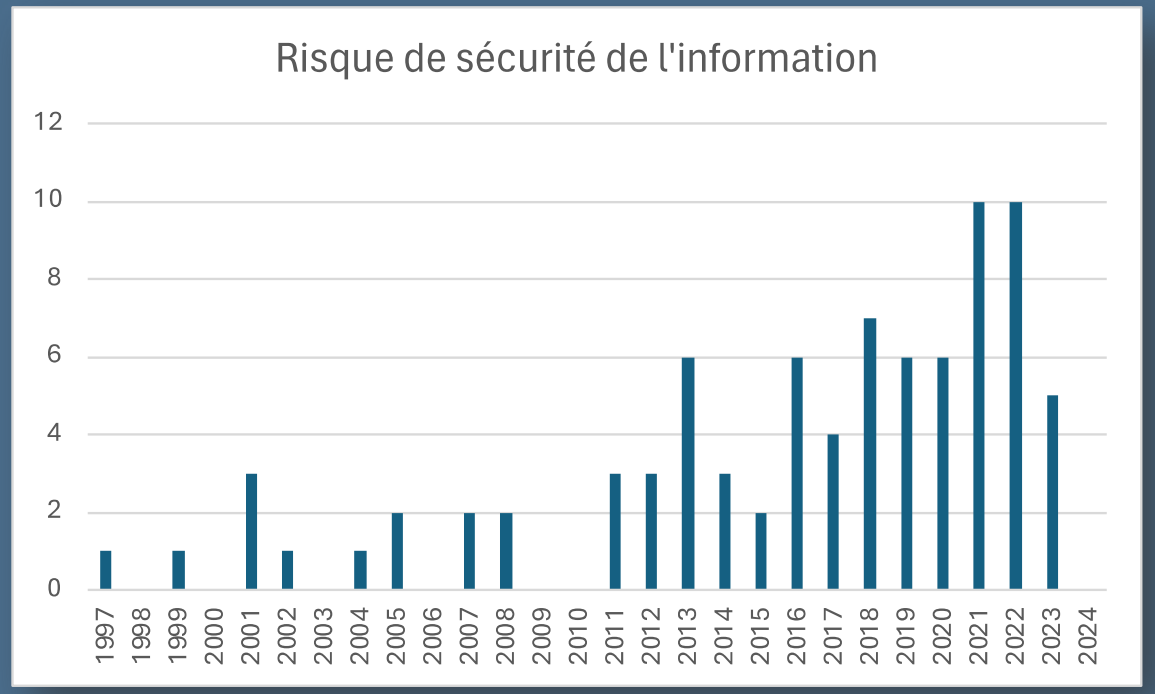
Résultats

Résultats de la revue académique

# Le risque pour la sécurité de l'information
n = 84

Catégories	Descriptions et sous-catégories	Nombre d'article
Evaluation des risques	Méthodes d'évaluation quantitatives et/ou qualitatives des risques	51
Gestion des risques	Management, bonnes pratiques, contrôles de sécurité, mitigations, aide à la décision	27
Système cyber-physique	Smart city, secteur de la santé, pipeline, objets connectés, secteur de l'énergie, usines de production chimique	21

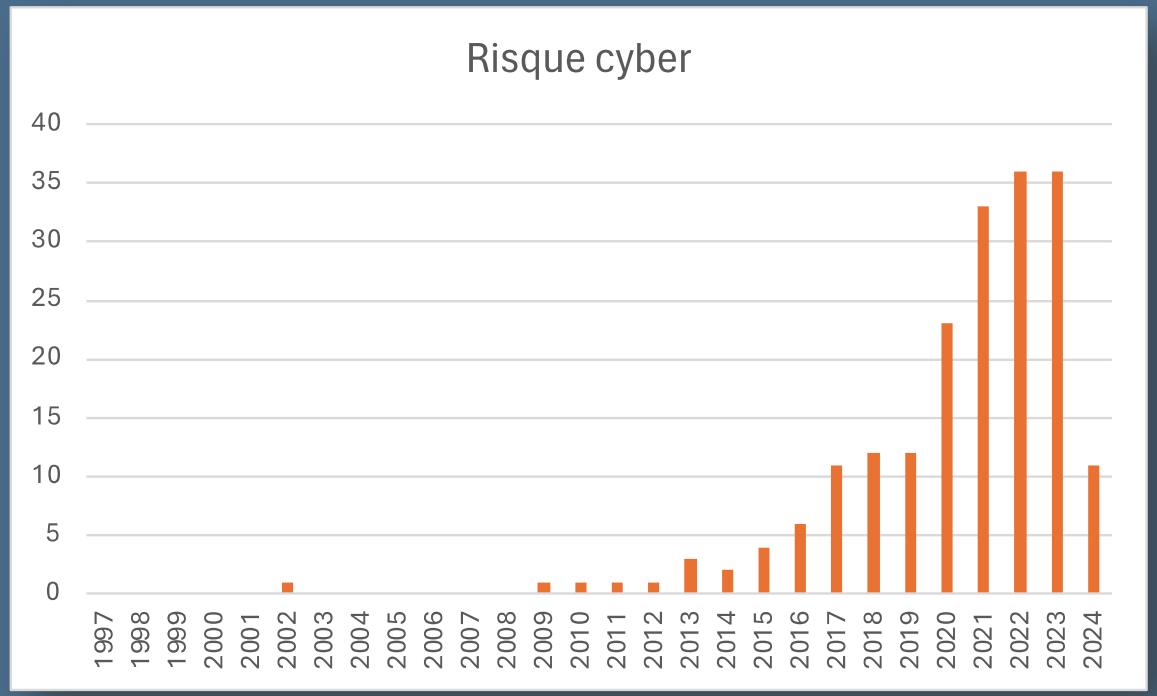
Evolution chronologique [1997 ; 2023]



Le risque de cyber
n = 193

Catégories	Descriptions et sous-catégories	Nombre d'article
Gestion des risques	Management, bonnes pratiques, contrôles de sécurité, mitigations	83
Evaluation des risques	Méthodes d'évaluation quantitatives et/ou qualitatives des risques	74
Systèmes cyber-physique	Infrastructures critiques, secteur de l'énergie, eau, pipeline, objets connectés, secteur maritime, secteur de la santé, secteur du transport	72
Caractéristiques du risque	Dynamique, sociotechnique, systémique, multi-dimensionnel, incertitude	52

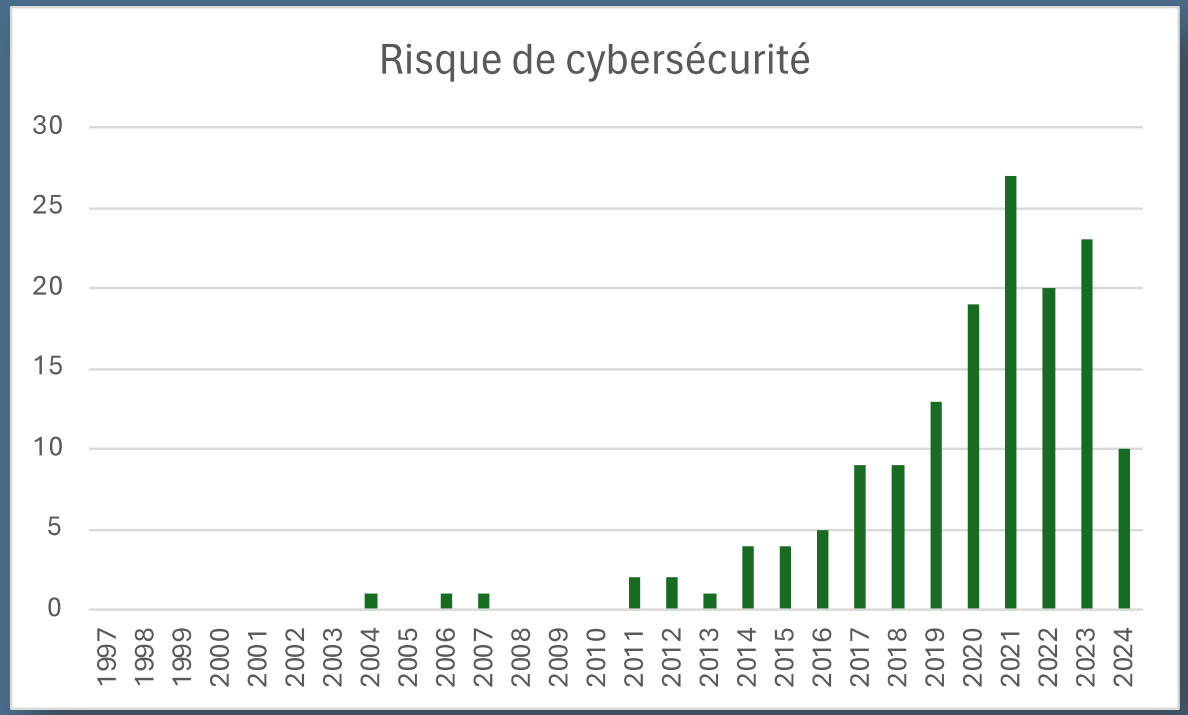
Evolution chronologique [2002 ; 2024]



# Le risque de cybersécurité
n = 151

Catégories	Descriptions et sous-catégories	Nombre d'article
Gestion des risques	Management, bonnes pratique, contrôles de sécurité, mitigations aide à la décision	64
Evaluation des risques	Méthodes d'évaluation quantitative et/ou qualitatives des risques	57
Systèmes cyber-physique	Infrastructures critiques, secteur de l'énergie, eau, pipeline, secteur de la santé, secteur du maritime, objets connectés, secteur du transport, secteur de l'aviation, smartphones, système de contrôle industriel, smart city	49

Evolution chronologique [2002 ; 2024]



Résultats de la revue professionnelle

# Collecte des données
n = 111

Catégorie	Nombre
Instances gouvernementales et régaliennes	40
Groupements étatiques	14
Associations	14
Méthodes d'analyse du risque	12
Organisations, groupements d'organisations et coopérations	12
Frameworks	10
Normes	7
Autorités indépendantes	2

Collecte des données

n = 111

Zones géographique	Nombre
Europe	64
Amérique	22
Applicable à l'international	20
Asie	4
Australie et Nouvelle Zélande	1

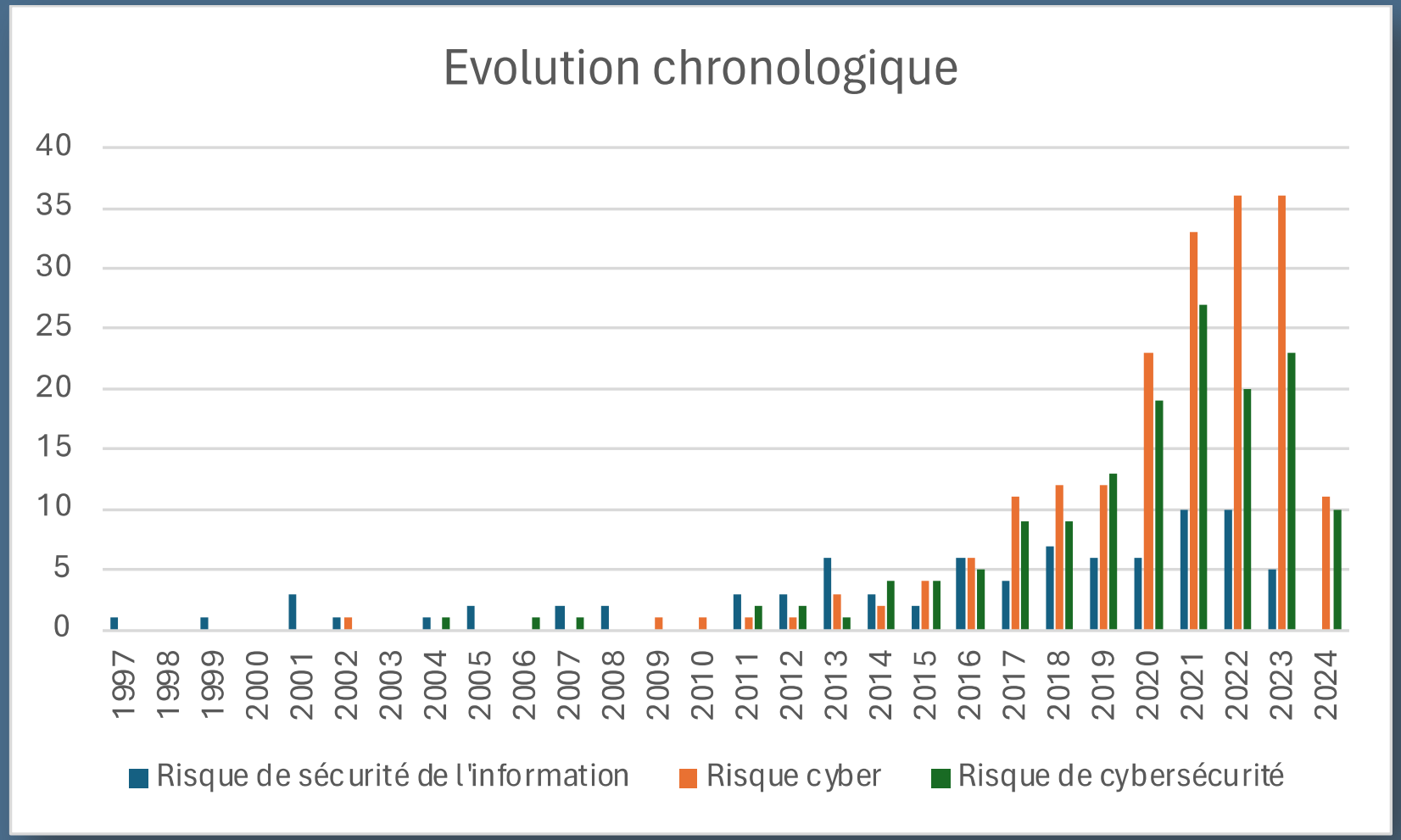
Analyse des données

37 termes différents

Catégorie	Termes les plus employés
Instances gouvernementales et régaliennes	Cybermenace, cybercriminalité et risque cyber
Groupements étatiques	Cybermenace, cybercriminalité et risque cyber
Associations (toutes françaises)	Risque cyber
Méthodes d'analyse du risque	Risque cyber
Frameworks	Risque cyber
Organisations, groupements d'organisation et coopération	Risque cyber
Normes	Risque de sécurité de l'information
Autorités indépendantes	Risque pour les individus

Mise en perspective des revues

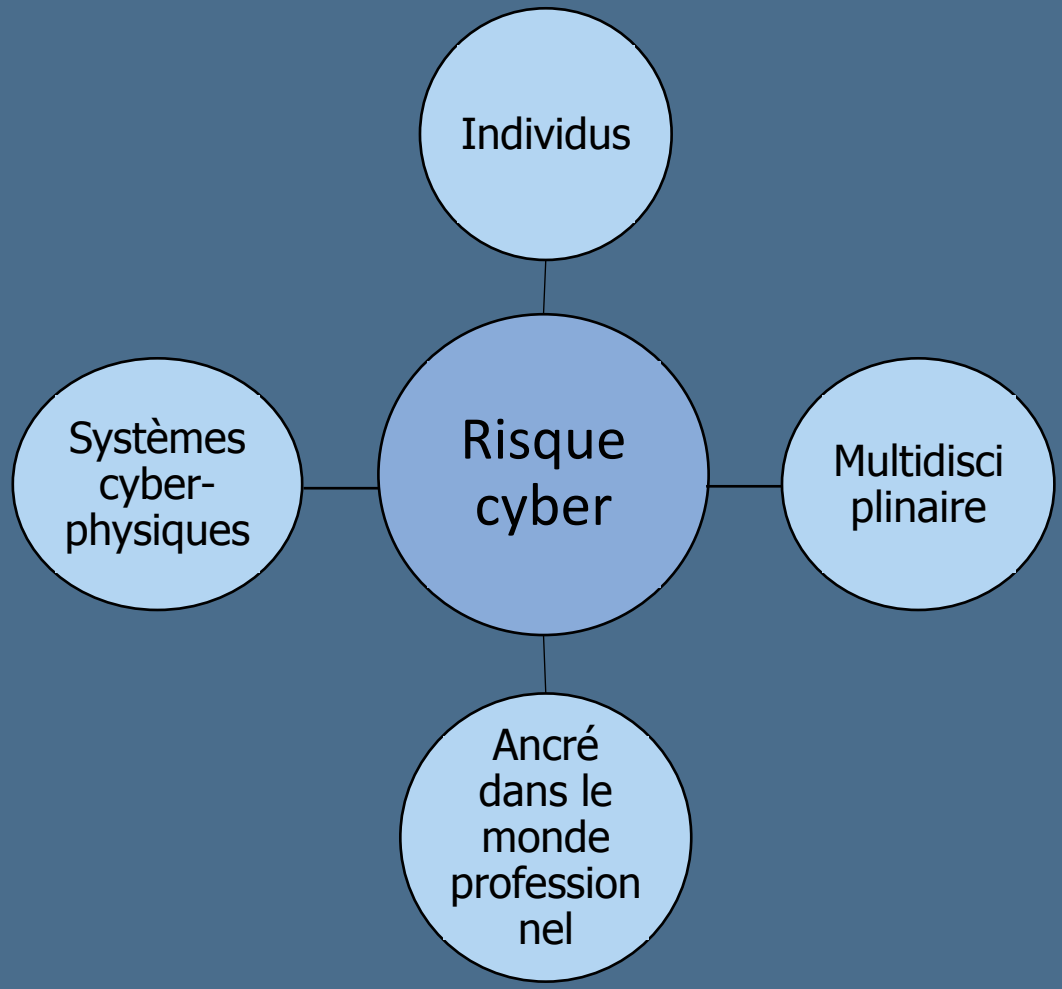
Une évolution d'usage chronologique



Une différence géographique

Zone	Composante « cyber »	Composante « information »	Autre
Europe	57%	11%	33%
Amérique	71%	21%	7%
International	45%	40%	5%

Un périmètre au-delà des actifs informationnels



Limites de cette recherche

Revue académique

Revue non-exhaustive.

La revue gagnerait à être plus approfondie.

Revue professionnelle

Revue esssentiellement européenne et francaise.

Revue non-exhaustive

Revue académique

Revue non-exhaustive.

La revue gagnerait à être plus approfondie.

Revue professionnelle

Revue esssentiellement européenne et francaise.

Revue non-exhaustive

Recommandations pour de futures recherches

Recommandations pour de futures recherches

Réalisation d'une cartographie de l'écosystème cyber.

Redéfinition multidisciplinaire et proposition d'un cadre universel du risque cyber.

Redéfinition des bordures et des périmètres entre les risques cyber et pour la sécurité de l'information.

L'emploi de paradigme de recherche tels que la DSR afin de réduire l'écart entre les milieux professionnels et académiques.

Des questions ?