PROJET MERCURIE

Évaluation de l'impact des cyberattaques sur l'économie française

École de Guerre Économique & Agora 41 · Promotion 2025 - 2026

Mattias Allio · Théo Gapihan · Baudouin Pedro-Rousselin · Élie Mimerane · Godefroy Sulger

PRÉSENTATION

Responsable MercurIE
Coach

Patrick CANSELL

Donneur d'ordres
Agora 41

Philippe LAVAULT

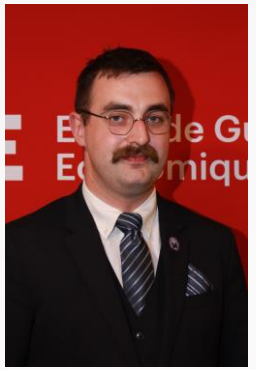
L'équipe

Théo GAPIHAN

Baudouin PEDRO-ROUSSELIN

Elie MIMERANE

Mattias ALLIO



Godefroy SULGER

PÉRIMÈTRE

Ce que l'on appelle cyberattaque

Définition retenue dans l'étude

Une cyberattaque est un acte malveillant visant un système d'information, des données ou des services connectés, dans le but d'en compromettre la disponibilité, l'intégrité, l'authenticité ou la confidentialité.

EXEMPLES DE TYPOLOGIES D'ATTAQUES TRAITÉES

- Rançongiciels
- Hameçonnage
- Piratage de compte
- Exfiltration de données
- Déni de service (DDoS)
- Fraude au virement

INTRODUCTION

Menace visible, coût mal mesuré

ANSSI 2024 : une année marquée par les **attaques d'extorsion, d'espionnage et de déstabilisation**

Une **menace** qui se généralise désormais à **toutes les tailles d'entreprises**

Coûts directs (remédiation, RH, communication) et **coûts indirects** (interruption, pertes commerciales, réputation, contentieux)

420 000

demandes d'assistance d'entreprises et d'associations à Cybermalveillance.gouv.fr en 2024 (+24 %)

47 %

des entreprises déclarent avoir subi au moins une cyberattaque significative (baromètre CESIN 2024)

26 % vs 44 %

26 % des organisations françaises disposent d'un plan de prévention ET de réponse (McAfee 2016)

INTRODUCTION

Pourquoi le coût reste un angle mort

Pas d'évaluation nationale homogène

Aucun dispositif public de collecte récurrente et homogène du coût économique

Sous-déclaration des incidents

Le chiffre caché de la cybercriminalité : la crainte réputationnelle et sécuritaire

Effets indirects insaisissables

Réputation, désorganisation et pertes à long terme échappent largement à la mesure

Recommandation n°4 de la Cour des Comptes *« mettre en place à court terme un observatoire de la cybermenace »* chargé de centraliser, à l'échelle nationale, données et analyses.

INTRODUCTION

Enjeux et méthodes

Enjeux

Combien les cyberattaques coûtent-elles réellement à l'économie française chaque année ?

Un ordre de grandeur exploratoire

Nous ne défendons pas un chiffre au centime près, mais méthodologie qui aboutirait à des chiffrages qui peuvent être consolidés

UNE DÉMARCHE EN DEUX TEMPS

1. **À partir des données existantes :** État de l'art en sources ouvertes, puis transposition au cas français
2. **À partir d'une enquête de terrain :** Un questionnaire et trois méthodes d'estimation nationale

INTRODUCTION

Résultat de l'étude

96,1 Md€ en 2025

≈ 3,3 % du PIB français

PARTIE I

Chiffrage en sources ouvertes

État de l'art international, facteurs impactant l’ampleur d'une attaque, puis transposition au cas français

PARTIE I · ÉTAT DE L'ART

État de l'art : un recensement en sources ouvertes

SOURCES MOBILISÉES

- Des sources variées
  - **Typologie** : think tanks, entreprises, organes étatiques
  - **Temps** : 2011 - 2025
  - **Espace** : Singapour, États-Unis, Israël

27 lignes « nationales »	**33** lignes « par attaque »
2 sources françaises	**4** sources françaises

EXEMPLES DE SOURCES MOBILISÉES

Cour des Comptes	**Asterès**	**Besse**
Bitkom	**Statista**	**IBM / Ponemon**

Données recensées sur chaque ligne de l'Excel

- Coût (en million de devise)
- Devise
- Période concernée par le chiffre
- Structure (pays, GE, TPE/PME…)
- Échelle (par attaque / globale)
- Pays concerné
- Source et source mère éventuelle
- Commentaires

PARTIE I · FACTEURS D'INFLUENCE

Les facteurs influençant l'impact des cyberattaques

FACTEUR PRINCIPAL : LA TAILLE

Coût moyen par attaque réussie (en € pour l'année 2025)

TPE	250 000
PME	460 000
ETI	3 360 000
Grande entreprise	23 960 000

Cour des Comptes : 5 à 10 % du chiffre d'affaires de l'organisation touchée

Secteur d'activité : Finance, énergie et technologies plus exposés (dépendance au SI, données sensibles)

Typologie d'attaque : Arnaques et paralysies de SI sont les plus coûteuses (KPMG)

Interconnexion : Une attaque se propage entre partenaires (NotPetya), phénomène d'immunité collective

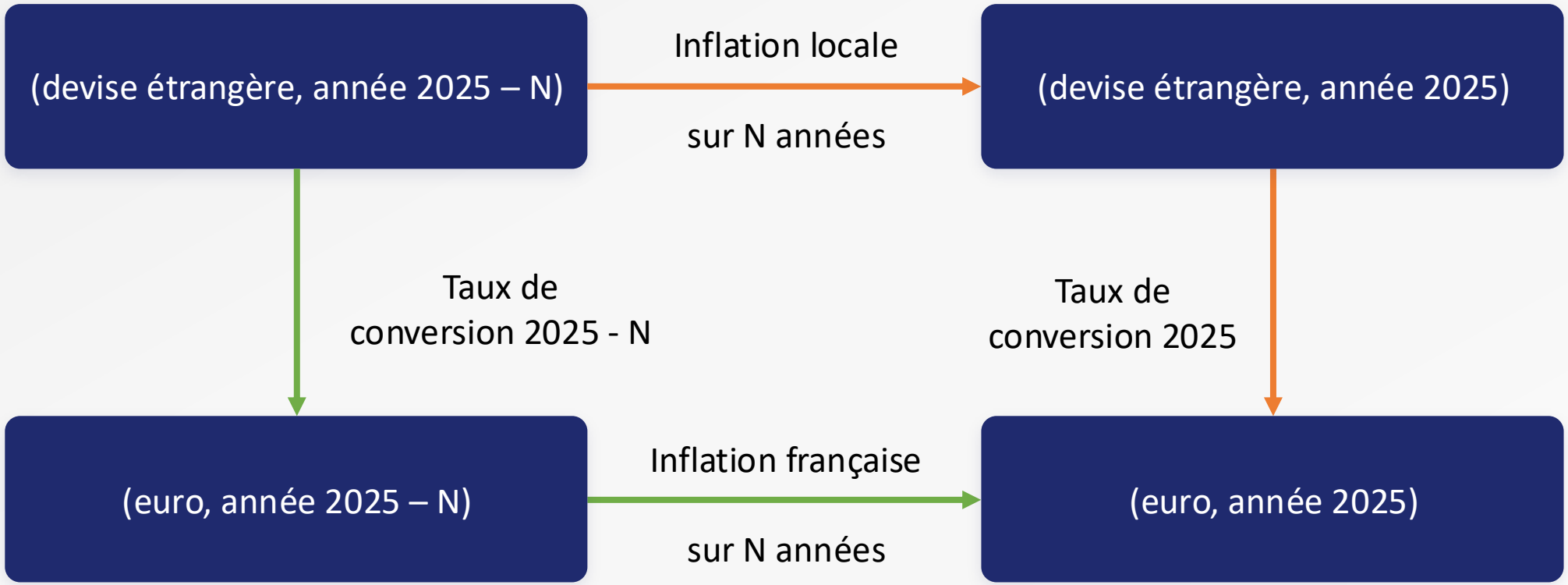
Coûts de transfert : Toute perte d'entreprise n'est pas une perte nationale (report vers un concurrent FR)

Géopolitique : Exposition liée au poids diplomatique (pic d'attaques pendant les JO de Paris 2024)

PARTIE I · MÉTHODOLOGIE DE TRANSPOSITION

Transposer les chiffrages étrangers à la France

Situation de référence : France en 2025



PARTIE I · MÉTHODOLOGIE DE TRANSPOSITION

Correction en fonction de l'intensité de l'activité économique

L'impact des cyberattaques dépend de l'intensité de l'activité économique
Il faut appliquer une dernière **transposition pour adapter les échelles des économies**

Par le PIB

Compare les économies à l'échelle macroéconomique globale.

Par le chiffre d'affaires

Rapporte le coût à l'intensité de l'activité économique des entreprises

Par la valeur ajoutée

Ramène à la richesse réellement produite par l'économie.

La comparaison entre pays suppose des **structures économiques proches**

PARTIE I · EXEMPLE DÉTAILLÉ

Cas d'étude : estimation allemande de Bitkom

Bitkom : **202,4 Md€ en 2025** pour l'économie allemande

→On applique les 3 méthodes

Exemple : rapport des PIB

202,4 Md€ — Coût estimé pour l'Allemagne (Bitkom)

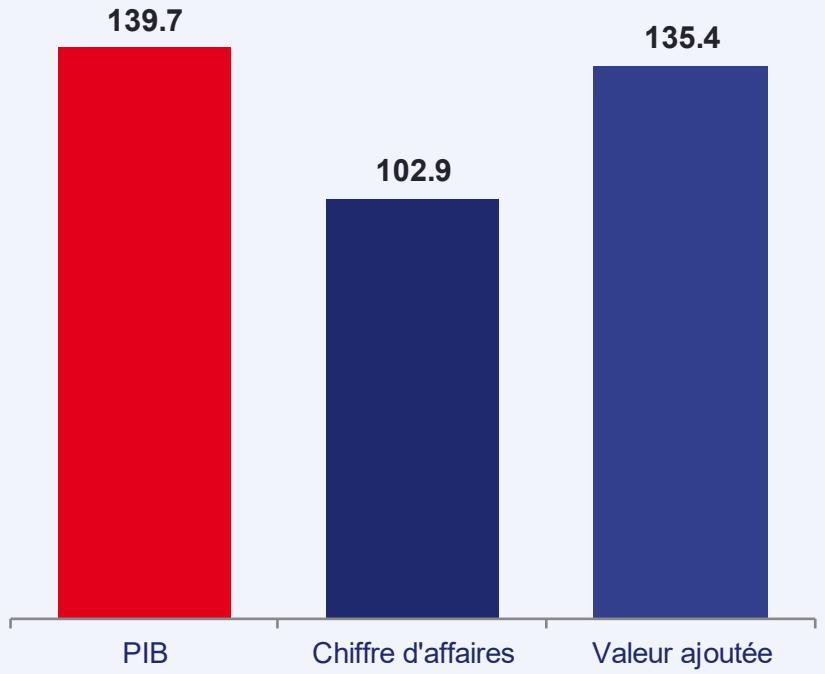
↓

× 67,5 % — PIB France (3 160 Md$) ÷ PIB Allemagne (4 686 Md$)
Source : Banque Mondiale 2024

↓

= 139,7 Md€ — Coût transposé à la France (méthode PIB)

LE MÊME CAS, SELON LES 3 MÉTHODES



PARTIE I · RÉSULTAT DE LA PREMIÈRE MÉTHODOLOGIE

Généralisation aux 27 chiffrages

La même **transposition par le PIB** est appliquée aux **27 chiffrages nationaux recensés**

MOYENNE DES 27 SOURCES (MÉTHODE PIB)

87,6 Md€ en 2025

PARTIE I · LIMITES

Faible échantillonnage et fiabilité des sources

Faible échantillonnage

Structure	Coût (en 2025) (M€)	Echantillon
TPE	0,249	3
PME	0,458	4
ETI	3,36	5
GE	23,96	17

Fiabilité des chiffrages

€ **Conflits d'intérêt :** Une dizaine de chiffrages proviennent d'entreprises offrant des solutions informatiques (IBM, McAfee, Microsoft, Norton)

Hétérogénéité des chiffrages : Préjudice déclaré vs estimations
Périmètre des études (définition des cyberattaques, coûts étudiés)

PARTIE II

Estimation par collecte de données

Mesurer directement : les difficultés de collecte, la typologie des coûts retenue, puis trois méthodes d'estimation nationale

PARTIE II · CONSTRUCTION D'UN QUESTIONNAIRE

Construire un outil d'enquête pertinent :

Prendre en compte les difficultés inhérentes à la matière cyber (1/2).

1. **Une donnée sensible et intéressant directement la sécurité de l'entreprise :** La communication sur un incident cyber peut fournir des informations utiles aux attaquants tout en affectant l'image de l'organisation

→ Dès lors, le questionnaire ne peut demander des montants précis, mais doit proposer des **intervalles** et des **ordres de grandeur** afin d'inciter les entreprises à répondre

PARTIE II · CONSTRUCTION D'UN QUESTIONNAIRE

Construire un outil d'enquête pertinent :

Prendre en compte les difficultés inhérentes à la matière cyber (2/2)

2

Un coût en grande partie dissimulé : 90 % de l'impact total d'une cyberattaque est constitué de coûts cachés

Source : **Deloitte,** ***Beneath the surface of a cyberattack: A deeper look at business impacts,*** **2016**

Un constat : 58 % des TPE-PME ne disposent d'aucune estimation chiffrée de l'impact d'une attaque

Source : **OpinionWay pour Cybermalveillance.gouv.fr,** ***Mesure de notoriété et de maturité en matière de cybersécurité auprès des TPE-PME,*** **2025**

Dès lors, le questionnaire ne peut se contenter de demander une estimation globale mais doit guider le répondant au travers une typologie de coûts

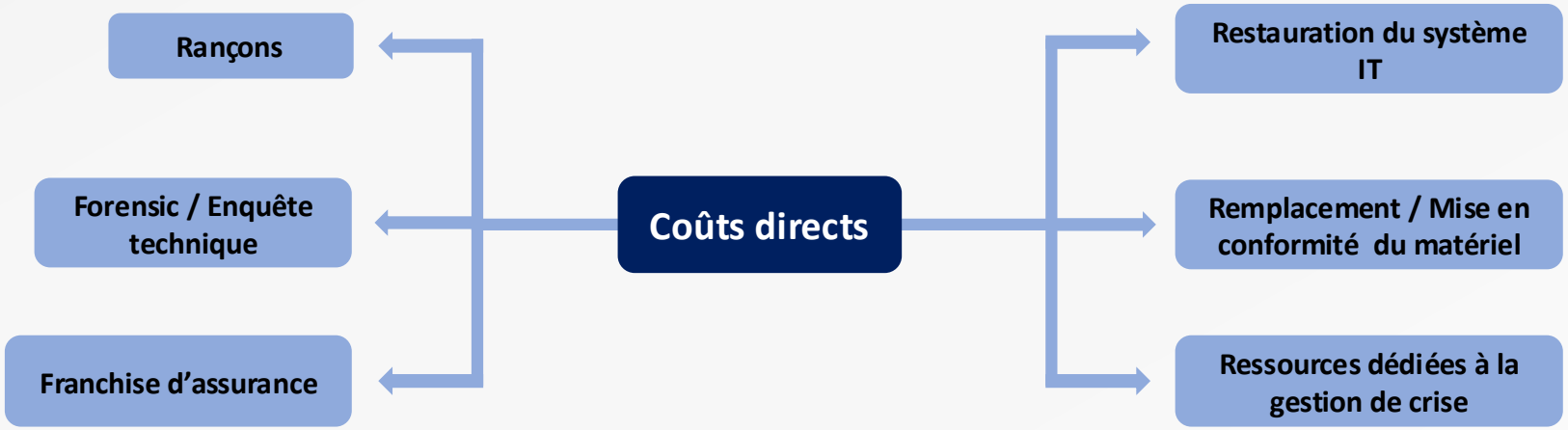
PARTIE II · CONSTRUCTION D'UN QUESTIONNAIRE

Construire un outil d'enquête pertinent :

Proposer une typologie d'analyse complète (1/2)

Coûts directs : Dépenses engagées par l'organisation pour répondre à l'incident, en assurer la gestion et restaurer son fonctionnement

Les coûts directs sont généralement immédiats, identifiables et directement imputables à l'incident



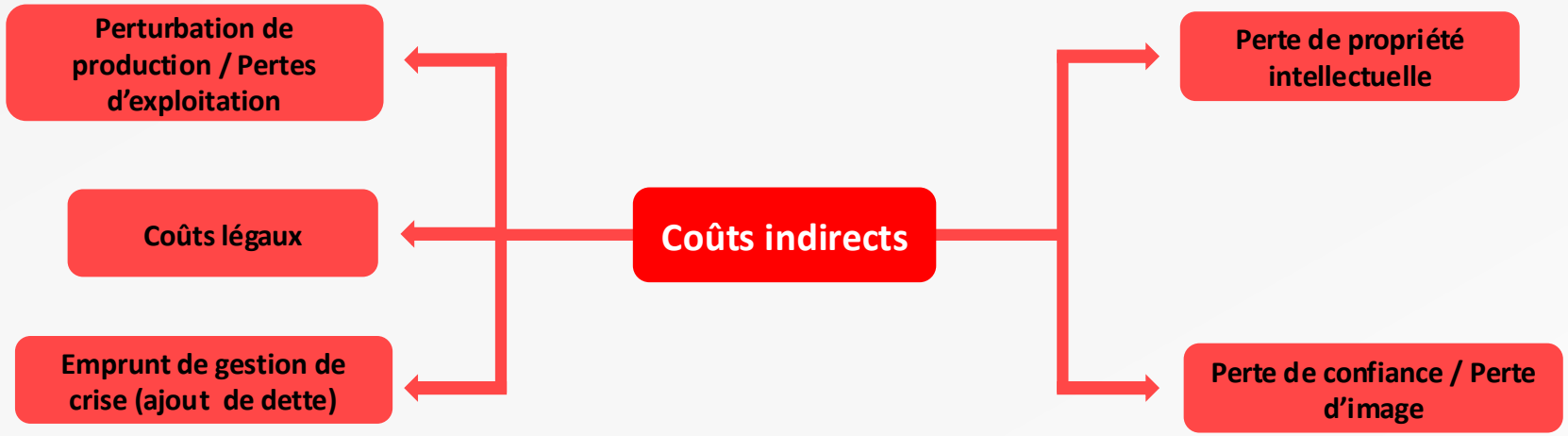
PARTIE II · CONSTRUCTION D'UN QUESTIONNAIRE

Construire un outil d'enquête pertinent :

Proposer une typologie d'analyse complète (2/2).

Coûts indirects : Conséquences économiques que l'attaque produit au-delà de l'événement lui-même

Les coûts indirects sont plus diffus, différés et souvent plus difficiles à rattacher avec certitude à la cyberattaque qui les a déclenchés



PARTIE II · MÉTHODES D'ESTIMATION

Trois méthodes d'estimation indépendantes

1

Taille & chiffre d'affaires

L'impact est rapporté au chiffre d'affaires de l'entreprise, puis projeté par catégorie de taille au PIB Français

93,9 Md€

2

Approche sectorielle

Le coût d'une entreprise est rapporté au poids de son secteur, puis extrapolé

100,5 Md€

3

Modèle assurantiel

Une simulation Monte-Carlo de 5 M d'entreprises intègre l'incertitude

102,6 Md€

PARTIE II · MÉTHODES D'ESTIMATION

Trois méthodes d'estimation indépendantes

1

Taille & chiffre d'affaires

Fiche d'identité PME 850 K€ de CA

Chiffre d'affaires de l'entreprise
850 k €

Attaque Cyber
100k€
11,7%

PIB Français des PME
1 000 Md €

29 Md €
2,9 %

25% d'entreprises victimes de cyberattaques

PME	ETI
29 Md €	27Md €
TPE	GE
19 Md €	25 Md €

93,9 Md €

PARTIE II · MÉTHODES D'ESTIMATION

Trois méthodes d'estimation indépendantes

2

Approche sectorielle

Fiche d'identité Commerce – Distribution. 850 K€ de CA

Part du secteur dans le PIB Français

242 Md €

Chiffre d'affaires de l'entreprise

850 k€

Attaque Cyber
100 k€

CA de l'entreprise / chiffre d'affaire du secteur
0,0003499382462%

Extrapolation par le secteur Commerce - Distribution

81 607 437 593,51 €

25% d'entreprises victimes de cyberattaques

Extrapolation par le secteur Industrie

110 687 554 549,94 €

Extrapolation par le secteur Informatique

11 756 875 000,00 €

100,5 Md €

PARTIE II · MÉTHODES D'ESTIMATION

Trois méthodes d'estimation indépendantes

1. Partir des données observées

Coûts déclarés, tailles d'entreprises, secteurs, fréquence des attaques.

2. Calibrer les distributions

Fréquence des attaques + sévérité des pertes.

3. Simuler des milliers de scénarios

Pour chaque entreprise simulée : attaque ? si oui, coût tiré aléatoirement.

4. Lire la distribution des pertes

Espérance nationale, VaR, CVaR, événements extrêmes.

Exemple de simulation

Entreprise A	→	attaquée	→	120 k€
Entreprise B	→	non attaquée	→	0 €
Entreprise C	→	attaquée	→	850 k€

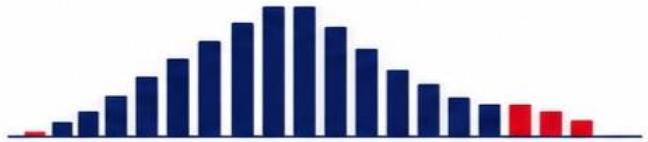
1 tirage aléatoire = 1 scénario

Répéter l'opération

Scénario 1
Scénario 2
Scénario 3
...
Scénario 10 000

On répète la simulation des milliers de fois

Distribution finale



Certaines pertes sont faibles, d'autres extrêmes

Espérance | VaR | CVaR

Hypothèses clés

- Taux d'attaque retenu : 40 %
- Portefeuille simulé : 5 millions d'entreprises
- Données INSEE + questionnaire

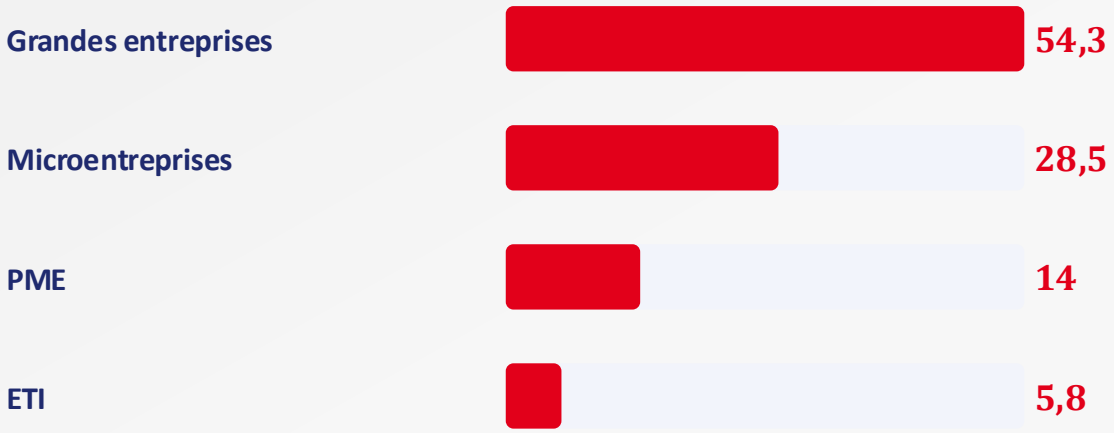
102,6 Md €

PARTIE II · LECTURE DES RÉSULTATS

Où se concentre le coût ?

Le coût projeté ne se répartit pas uniformément : il se concentre sur certaines tailles d'entreprise et certains secteurs

PAR TAILLE D'ENTREPRISE (modèle assurantiel, Md€)



Les grandes entreprises portent l'essentiel en valeur absolue ; les microentreprises pèsent par effet de masse

PAR SECTEUR (Md€)

Une charge transversale. Le risque cyber est diffus et systémique

CONCLUSION

Portée, limites et recommandations

96,1 Md€ en 2025

soit ≈ 3,3 % du PIB français

CONCLUSION · PORTÉE ÉCONOMIQUE

Les cyberattaques, une « maladie » économique

Des marges rognées

Le coût des attaques et de la protection pèse directement sur la rentabilité des entreprises

De l'investissement détourné

Des ressources qui financeraient l'innovation et la productivité partent en remédiation

Un effet de masse

Concentré sur les grandes entreprises en valeur, le coût frappe aussi les microentreprises par leur nombre

Invisible mais bien réelle : parce que diffuse, cette charge n'apparaît dans aucune ligne comptable nationale

CONCLUSION · PORTÉE ÉCONOMIQUE

Un risque de continuité économique nationale

Un risque systémique

Chaînes de sous-traitance fragilisées

Une attaque chez un fournisseur se propage à toute une filière

Un enjeu de compétitivité

Le surcoût pèse sur la position des entreprises françaises face à leurs concurrents

Un enjeu de souveraineté

La protection des secteurs stratégiques devient une question d'intérêt national

« **Le risque cyber n'est pas seulement un risque informatique : c'est un risque pour la sécurité économique nationale.**

CONCLUSION · TRANSPARENCE MÉTHODOLOGIQUE

Les limites à garder à l'esprit

Un ordre de grandeur, pas une mesure exacte

La valeur du chiffre est d'indiquer l'ampleur économique du phénomène, pas de la trancher au centime près

Échantillon restreint

Cinq réponses qualifiées : une preuve de concept, non un échantillon représentatif

Hypothèses fortes

Taux d'incidence et d'attaque (25 % / 40 %), structures économiques comparables

Transposition fragile

Comparer des économies suppose des structures et des entreprises réellement proches

Sensibilité au modèle

Le résultat dépend beaucoup des hypothèses initiales ainsi que de la modélisation du portefeuille d'entreprise

CONCLUSION · INDUSTRIALISER LA COLLECTE

Combien de réponses pour fiabiliser ?

5

AUJOURD'HUI

Preuve de concept : tester et valider les méthodes

385

MINIMUM

Seuil statistique global pour une première mesure crédible

1 000

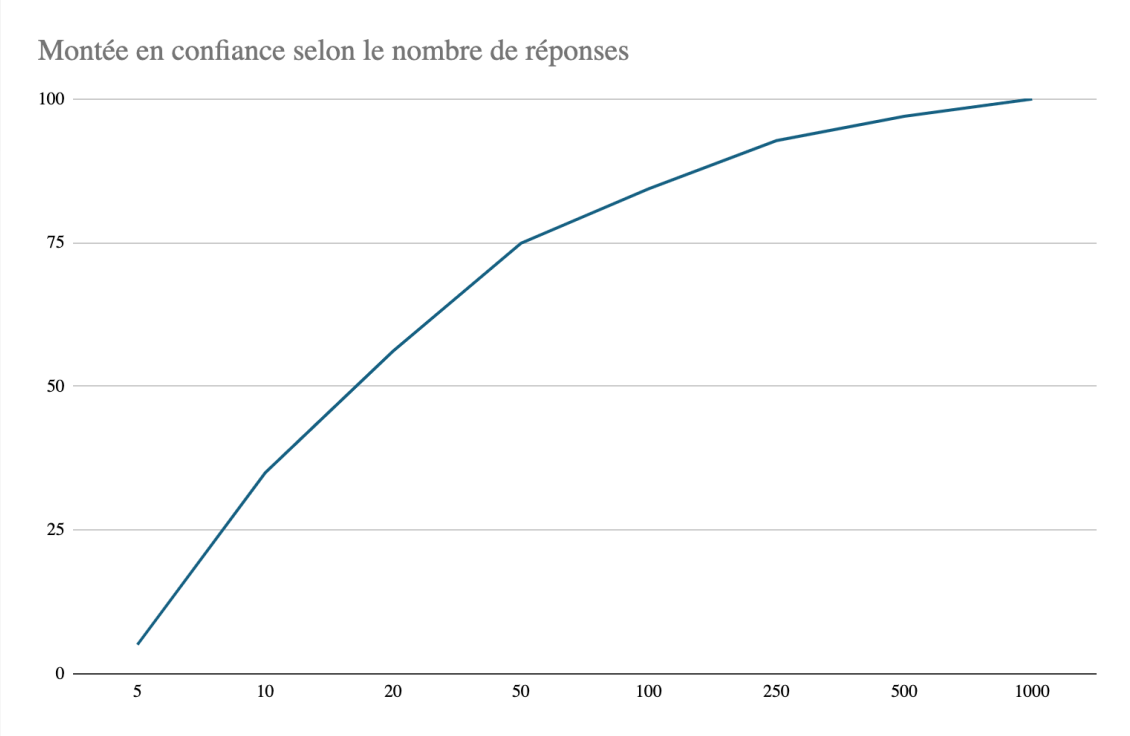
RECOMMANDÉ

Analyse robuste par taille et par secteur

2 000+

CIBLE

Analyse fine par type d'attaque



CONCLUSION

Un retard français à combler

À l'inverse de nombreux partenaires, la France ne dispose d'aucun rapport, ni d'aucune structure mesurant ces coûts de manière récurrente.

France

Aucun dispositif national, public et structuré, ne mesure le coût des cyberattaques de façon récurrente. Ce rapport propose un cadre méthodologique et un premier chiffrage consolidé pour y remédier.

AILLEURS, DES DISPOSITIFS DÉJÀ ANCIENS

- **États-Unis** IC3 depuis 2001 · Ponemon 2009 · CISA/Cyentia 2022
- **Royaume-Uni** Oxford/CPNI dès 2014 · KPMG en 2025
- **Allemagne** Bitkom : chiffrage annuel depuis 2015
- **Italie** Banca d'Italia depuis 2017
- **Japon** Police recense les préjudices déclarés

CONCLUSION · RECOMMANDATION 1 / 3

Créer un observatoire dédié

1

En l'absence d'organisme public sur le sujet, l'Agora 41 pourrait porter un observatoire des coûts des cyberattaques, structuré autour de trois pôles

1

Collecte des données

Veille en sources ouvertes et approfondissement académique

2

Traitement & analyse

Diffusion et exploitation d'un questionnaire standardisé

3

Communication

Sensibiliser entreprises et fédérations et nouer des partenariats durables

CONCLUSION · RECOMMANDATION 2 / 3

Généraliser l'obligation de signalement

2

Instaurer une déclaration structurée des cyberattaques, dans l'esprit d'une déclaration d'accident du travail, pour produire des données homogènes et exploitables

1

Formulaire unique

Renseigné lors de l'incident : nature, conséquences et coûts associés

2

Typologie commune

Une grille partagée des coûts et des types d'attaques

3

Données comparables

Condition de statistiques fiables et suivies dans le temps

CONCLUSION · RECOMMANDATION 3 / 3

Créer un guichet unique

3

Face à la dispersion des acteurs publics, un guichet unique national améliorerait à la fois le parcours des victimes et la connaissance du phénomène

1

Orientation des victimes

Un point d'entrée simple pour particuliers et organisations de toute taille

2

Base de données centralisée

Recenser les déclarations au sein d'une base unifiée

3

Vision d'ensemble

Donner à l'État une vue nationale, aujourd'hui éclatée entre structures

EN UN MOT

Le coût des cyberattaques reste largement sous-estimé et insuffisamment mesuré

Trois méthodes indépendantes convergent vers un ordre de grandeur proche de 100 milliards d'euros par an. Cela suffit à établir que le cyber n'est plus un risque marginal ou purement technique : c'est un enjeu économique national.

Mieux sensibiliser

Réduire l'exposition des entreprises, de toutes tailles

Mieux mesurer

Chiffrer les dommages pour piloter les politiques publiques

PROJET MERCURIE

Merci pour votre attention

La cybersécurité, un enjeu économique national

Mattias Allio · Théo Gapihan · Baudouin Pedro-Rousselin · Élie Mimerane · Godefroy Sulger