Risques systémiques: Assurance et Résilience

Cyber-Risques Systémiques

Dr. Corneille KAREKEZI

Directeur Général du Groupe

Société Africaine de Réassurance

Présentation à la 46ème FANAF | 23 Mai 2022 (Dakar, Sénégal)

Risques systémiques

L'expression **"Risques systémiques"** désigne (en assurances) des risques dont l'**ampleur** est telle qu'ils **peuvent engendrer, sur le plan économique et sociétal**, des pertes d'un niveau suffisamment élevé pour provoquer l'**effondrement de tout un système**. A la différence des risques catastrophiques typiques, les risques systémiques **ont un impact ressenti simultanément par une partie si importante de la société, dans de zones géographiques si différentes, des industries et branches d'assurance si variées**, que les **mécanismes traditionnels de transfert du risque deviennent inadaptés, compte tenu du fait que le risque ne peut être ni mutualisé ni absorbé efficacement**. Ils débordent des limites traditionnelles du risque. Du fait des contraintes d'assurabilité, le coût est pris en charge par le gouvernement, ce qui entraîne un impact inattendu."

N.B.: D'autres 'risques systémiques' liés à l'économie ou en découlant, sont causés par les variations extrêmes et soudaines des **taux d'intérêt**, **des taux de change,** de la **performance des marchés financiers**, etc. Elles peuvent être dues à des facteurs économiques, politiques ou règlementaires, ou au comportement des acteurs du marché.

L'Evènement (Quoi?)

Il s'agit des éléments déclencheurs du risque systémique, pouvant prendre la forme de:

- Maladies infectieuses
- **Cyber-attaques**
- Evènements météorologiques extrêmes
- Guerres
- Crises financières

L'Etendue (Où?)

Il s'agit ici de l'ampleur et de l'échelle de la propagation au plan local, national, régional, continental et mondial en raison de la mondialisation:

- Interdépendance
- Interrelation
- Interconnexion

L'Effet (Pourquoi?)

L'on se réfère ici à l'effet de cascade, tant primaire que secondaire, de l'évènement. Par exemple, pour la Covid-19, les confinements sont un effet secondaire :

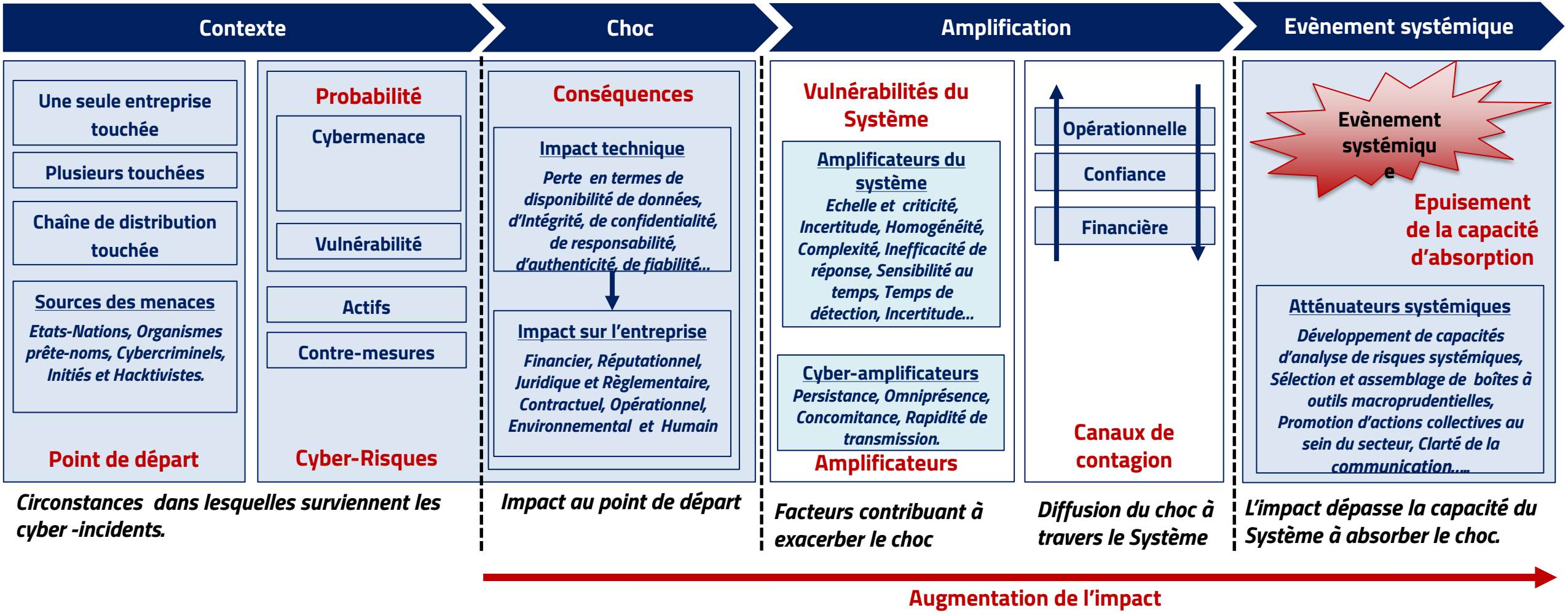
- Décisions du gouvernement
- Périls secondaires

L'Impact (Comment?)

Indique de quelle manière se manifeste l'impact final de cet évènement sur les individus, les entreprises et les gouvernements :

- Economique / Financier
- Politique
- Social
- Environnemental

Modèle des Cyber-Risques systémiques



NB: Tous les Cyber-Risques ne sont pas de nature systémique. Les cyber-risques systémiques ECHOUENT au test de l'assurabilité

Source: "The Making of a Cyber Crash – A Conceptual Model for System Financial Risks", ESRB Occasional Paper Series

Etude de cas de Cyber-Risques systémiques

Bashe Attack: Infection des systèmes mondiaux par un programme malveillant (ou 'Maliciel')

Il s'agit d'étudier un scénario dans lequel les **appareils des compagnies sont infectés par un maliciel** qui **menace de bloquer l'accès aux fichiers ou de les détruire si une rançon n'est pas payée**. L'attaque est lancée par le biais d'un **courriel infecté** qui, une fois ouvert, est transmis à l'ensemble des contacts et, en **24 heures,** crypte toutes les données de près de **30 millions d'appareils** dans le monde, ciblant plus de **600 compagnies**. Cette attaque rappelle celles de 2017, connues sous les noms de **WannaCry et NotPetya**.

'Bashe Attack': Une infection à l'échelle mondiale par un maliciel contagieux					
Pertes économiques (en milliards USD)		Pertes assurées (en milliards USD)		Niveau de couverture (%)	
Grands sinistres	Sinistres extrêmes	Grands sinistres	Sinistres extrêmes	Grands sinistres	Sinistres extrêmes
85	159	10	27		

1. **Couverture :** Pertes d'exploitation normales ou celles liées à la carence des fournisseurs, Cyber-Extorsions, Coût de réponse aux incidents et Cyber-responsabilité personnelle.
2. **Hypothèse** : Les pertes d'exploitation sont le facteur principal des pertes assurées, pour cette étude de cas. Scénario de 71% de sinistres majeurs et 59% de sinistres extrêmes. Les polices traditionnelles sans clause d'exclusion explicite sont considérées comme des **cyberpolices non-affirmatives**.
3. **Estimation** : Pour 2019, la prime d'assurance globale enregistrée au titre des **cyberpolices affirmatives** *(cyberpolices autonomes et avenants aux polices traditionnelles)* s'élève à 6,4 milliards USD, ce qui fait que l'estimation des pertes de l'industrie des assurances représente 1,2 à 3,4 fois la prime annuelle. **Cela montre que le secteur est fortement exposé au risque de contagion lié à un maliciel**.

"la prochaine pandémie avec une exposition semblable à celle d'**un virus biologique** sera de nature cybernétique, car n'étant soumise ni à la géographie ni au temps" - *International Insurance Executive.*

Le moment est venu de renforcer la cyber-résilience pour l'avenir. Selon les rapports publiés, en 2018, le coût de la cybercriminalité a été estimé à 0,2% du PIB pour l'Afrique et 0,8% du PIB mondial

Source: Cambridge Centre for Risk Studies

Digitisation et Sécurité Informatique

Africa Re a adopté VM Ware sur Amazon Public Cloud en 2020 pour son centre de données principal (Royaume-Uni) et son site de reprise après sinistre (États-Unis d'Amérique).

Elle a aussi investi dans plusieurs outils de sécurité informatique..

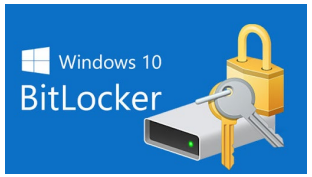
TREND MICRO

Antivirus Software

gemalto
security to be free

2 Factor Authentication

Remote Connection



Device Data Encryption

Intune

Mobile Device Management

Office 365

Collaboration Software

CYBERARK

Network Access Control

Virtual Desktop Connection

C'est la course à la sécurité informatique à coût de millions de dollars pour s'assurer que lorsque le risque tant attendu sera une réalité, nos sociétés puissant s'en tirer avec pas ou peu de dégâts.

Assurance desRisques Cybernétiques

RESPONSABILITE CIVILE

- Vie Privée et Divulgation des Données Cinfidentielles
- Responsabilité Civile Médias
- Pénalités et Coûts Réglementaires
- Pénalités Contractuelles

PERTE D'EXPLOITATION ET CRIMES CYBERNETIQUES

- Pertes d'Exploitation
- Ôûts de Restoration des Données et Systèmes
- Vols Informatiques
- Cyber Extorstion (Ransomware)

SERVICES INTEGRES

- Communication en cas de Crime Cybernétiques
- Dépenses d'urgences
- Frais de Consultations (Experts Informatiques et en Relations Publiques)

Discovery Period	Up to **60 Days**
Geographical Scope	**Worldwide** (Excluding United States of America and Canada)
Policy Limit	**US$ 10 Million** for Each and Every Loss and in the Aggregate
BI Maximum Indemnity Period	180 Days
Sub-Limits	**25%** Applicable to: Regulatory Costs and Fines; Hacker Theft Cover and Emergency Costs
Deductible	**Business Interruption and Restoration Costs**: **US$ 150 Thousand** | **Other Sections**: **US$ 50 Thousand**
Key Exclusions	**Dishonesty or Improper Conduct; Contractual Liability; Prior Claims and Circumstances; Trade Secrets and Intellectual Property; Bodily Injury and Property Damage; War; Terrorism and Governmental Actions; Unauthorised Collection of Data; Trading; Licensing Fees; Unauthorised Communications;**

Marché de l'Assurance Cyber-Risques

Cyber Menaces

01

Les cyber-menaces augmentent rapidement, stimulant la demande mondiale en réassurance.

Stimulé par la COVID-19, le **marché** mondial de la cyber-**assurance a progressé de 33,5% en 2020**. Les cyber-besoins évoluent rapidement et la (ré)assurance prend diverses formes, avec des couvertures pour l'extorsion, le piratage informatique, le vol en ligne et la destruction de données.

Taux de cession

02

Une part importante de la cyber-assurance africaine est cédée à des réassureurs sans appétit.

En 2021, le marché africain de la cyber-**assurance était évalué à un niveau situé entre 25 millions et 30 millions USD.** Les taux des cessions sont élevés car les assureurs cherchent à limiter leur cyber-exposition, conduisant à une **valeur totale de 20 millions USD pour le marché africain de réassurance**

Sensibilisation du Marché

03

Les services à valeur ajoutée jouent un rôle de plus en plus important sur le marché africain.

Les Ré(assureurs) offrent de plus en plus de services supplémentaires au titre de leur proposition de cyber-ré(assurance), y compris des cyber-services d'atténuation des risques et de réponse aux incidents. Toutefois, le marché de rétrocession est inexistant ou très limité.

Potentiel du Marché

05

Un potentiel important de progression existe encore sur le continent. Le déficit de protection est de 99,29%.

Eclairages

Le **coût engendré par la cybercriminalité, pour les économies africaines, s'est chiffré à 3,5 milliards USD** en 2017. Toutefois, un cinquième seulement des pays africains ont adopté un cadre juridique en matière de cybersécurité et 11 seulement ont adopté des lois relatives à la cyber criminalité

N.B.: Le **marché mondial de la cyber-assurance** est estimé à **10 milliards de dollars et progresse de 25% par an;** il devrait atteindre **21 milliards USD en 2025**.

Source: Africa Re Insights

Plan National de Résilience face aux Cyber-Risques systémiques

La "Cyber-résilience" concerne les mesures nécessaires à prendre afin d'**identifier les menaces et de se protéger contre elles , de détecter et de répondre aux incidents**, et de se **remettre rapidement d'une attaque**. La "Cyber-résilience est la capacité d'une organisation' à **fournir un niveau suffisant de services, en dépit de la survenance d'évènements indésirables**. Afin de maintenir cette **cyber-résilience**, l'organisation doit disposer d'un **programme formel d'information en matière de sécurité**, d'une **équipe dédiée** à cette tâche et d'un **système de gouvernance system** devant être intégrés aux **programmes en matière de risque, de poursuite des activités et d'éducation**" – *Sergio Ermotti (Chairman, Swiss Re)*

Résilience	Clients	Opérateurs du Secteur d'Assurances	Organismes gouvernementaux
Identifier et Protéger	• Conscientisation et Sensibilisation • Cadre de gouvernance • Due Diligence • Partenariat stratégique • Pratiques de GIRE • Investissements stratégiques • Gestion de la continuité des activités • Planification reprise après sinistre • Procédures opérationnelles standard	• Compétences techniques • Partenariats intersectoriels • Adéquation du Capital • Gestion de l'accumulation • Solutions innovantes • Solutions simplifiées • Pools d'assurance catastrophes • Collaborations au sein de l'industrie • Mesures d'Incitation pour les clients	• Plan stratégique national • Régime d'assurance obligatoire • Taux minimaux • Exigences de divulgation • Application de la Règlementation • Réformes sectorielles • Fournisseur de filet de sécurité • Régime d'assurance publique • Programmes de subvention
Détecter			
Répondre			
Se remettre			

Je vous remercie