

RAPPORT DU CLUB DES JURISTES

LE DROIT PÉNAL À L'ÉPREUVE DES CYBERATTAQUES

PRÉSIDENT DE LA COMMISSION

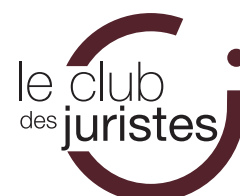
M. Bernard Spitz,
Président du pôle international et Europe du MEDEF,
Ancien président de la Fédération française de l'assurance (FFA)

SECRÉTAIRE GÉNÉRALE DE LA COMMISSION

Mme Valérie Lafarge-Sarkozy,
Avocate associée, cabinet Altana

CONTACT PRESSE

Guillaume Prigent
guillaume.prigent@leclubdesjuristes.com
06 68 68 22 11



LE RISQUE CYBER : UN POIDS ÉCONOMIQUE MAJEUR



**3^e ÉCONOMIE
MONDIALE**

c'est ce que serait le poids économique du risque cyber s'il était un pays, derrière les USA et la Chine⁽¹⁾



**190 000 DOLLARS
PAR SECONDE**

= le coût des attaques cyber⁽²⁾



10 500 MILLIARDS DE DOLLARS

= le coût du risque cyber s'il poursuit sa croissance annuelle de 15 % / an d'ici 2025 contre 3 000 milliards en 2015⁽³⁾

LES CIBLES PRIORITAIRES DES DÉLINQUANTS



**90%
DES ENTREPRISES**

ont constaté un incident de cybercriminalité en France en 2019, 43 % étant des PME⁽⁴⁾



8,6 MILLIONS €

= coût moyen par entreprise française des attaques numériques en 2018



NUMÉRO 1

c'est le classement du secteur public en nombre d'attaques reçues

DES MODES OPÉRATOIRES MULTIPLES



+148%

= taux d'augmentation des attaques par *ransomware* dans le monde entre février et mars 2020, soit une attaque toutes les 14 secondes



55% DES ATTAQUES

sont initiées par une organisation criminelle structurée



5\$

est le prix du kit accessible sur le darknet pour commettre une attaque cyber avec un rapport risque / coût / gain sans équivalent

LE DROIT PÉNAL À L'ÉPREUVE DES CYBERATTAQUES

Après un premier rapport en 2018 consacré à l'assurance du risque cyber, nous publions aujourd'hui le deuxième rapport de la commission « Cyber risk » du Club des juristes, consacré au traitement juridique des cyberattaques. Cette parution intervient dans un contexte de crise sanitaire et économique qui a eu pour conséquence une recrudescence de la cybercriminalité.

Si les évolutions numériques représentent pour les entreprises un véritable levier de croissance et de compétitivité, elles induisent une prolifération de risques nouveaux aux conséquences majeures. Les attaques cyber, qui pourraient coûter 6 000 milliards de dollars aux entreprises à travers le monde en 2021, démontrent la nécessité pour celles-ci d'adapter leur niveau de protection afin de limiter la vulnérabilité de leurs systèmes d'informations et de sécuriser leur patrimoine informationnel.

Une prise de conscience globale s'avère en effet indispensable. La cyber sécurité constitue un enjeu majeur pour les individus, les entreprises et les pays. Enjeu de protection de la vie privée et du patrimoine pour les citoyens ; enjeu de responsabilité en matière de données, enjeux financier et d'image pour les entreprises ; enjeu de souveraineté pour les pays. Pourtant, le nombre d'incidents en entreprise liés à la cybercriminalité ne cesse d'augmenter et l'ANSSI a traité entre 2019 et 2020 quatre fois plus d'attaques par rançongiciel. Il est urgent que les dirigeants dotent leurs entreprises d'une politique de cyber sécurité efficace, en même temps respectueuse de l'impératif de protection des données.

La justice pénale peut et doit accompagner ces mutations, notamment en simplifiant les procédures d'enquête sous pseudonyme dans le « darknet » et en incitant les victimes de cyberattaques à déposer plainte systématiquement, de manière à remonter et démanteler les filières plus rapidement. Il faudra, pour ce faire, allouer davantage de moyens humains et financiers à la lutte contre la cybercriminalité : renforcement des services de justice spécialisés, création d'une filière de cyber magistrats, approfondissement de l'offre de formation juridique en matière de cyber délinquance, etc.

Les 10 préconisations concrètes que nous formulons permettront de disposer des atouts essentiels de compétitivité et de souveraineté de notre pays dans le contexte des développements technologiques engagés au XXI^e siècle sur la voie du digital et de l'intelligence artificielle.

Président de la commission

M. Bernard Spitz,
*Président du pôle international et Europe du MEDEF,
Ancien président de la Fédération française
de l'assurance (FFA)*

Secrétaire générale de la commission

Mme Valérie Lafarge-Sarkozy,
Avocate associée, cabinet Altana

SYNTHÈSE DES RECOMMANDATIONS

À L'ATTENTION DU GOUVERNEMENT



1. FAIRE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ UNE CAUSE NATIONALE POUR 2022

- Lancer des campagnes récurrentes d'information et de sensibilisation ciblées par le biais des médias et réseaux sociaux, notamment avec le soutien des chambres de commerce, des compagnies et ordres professionnels
- Conclure un protocole entre le ministère de la Justice et la plateforme Cybermalveillance.gouv.fr

À L'ATTENTION DU MINISTÈRE DE LA JUSTICE



2. PROMOUVOIR LA FORMATION DES MAGISTRATS DU SIÈGE ET DU PARQUET ET LEUR FORMATION CONTINUE EN MATIÈRE DE CYBERCRIMINALITÉ

- Créer une filière de cybermagistrats, au besoin par le biais d'une formation diplômante
- Renforcer le pôle Cyber au niveau du parquet de Paris
- Renforcer la spécialisation d'une chambre du tribunal judiciaire en matière de droit du numérique et cybercriminalité
- Créer un département Numérique et Cyber au niveau de la cour d'appel de Paris, composé de magistrats du siège et du parquet
- Accentuer les formations communes ENM/EFB et Police / Gendarmerie / Douanes sur le droit du numérique et la lutte contre la cybercriminalité, avec des stages pratiques dans les services spécialisés
- Désigner un référent cyber par cour d'appel en actualisant régulièrement la liste



3. RENFORCER LA COOPÉRATION PUBLIC / PRIVÉ

- Orienter l'investissement public et privé vers l'émergence d'une filière française et européenne d'excellence en cyber technologie. Les plans d'investissements publics français et européens devraient favoriser le développement d'une filière européenne d'excellence dans le domaine de la cyber protection et accompagner les efforts du marché en faveur d'une réduction de la menace cyber.



4. ÉTOFFER LES SERVICES DE LA JUSTICE EN MATIÈRE DE LUTTE CONTRE LA CYBERCRIMINALITÉ

- Recruter des cadres et assistants spécialisés en matière de cyber sécurité, tant au niveau du tribunal judiciaire que de la cour d'appel de Paris
- Développer des échanges réguliers avec les compagnies des experts judiciaires
- Revoir la nomenclature des experts judiciaires, afin d'introduire une spécialité sur le numérique et la cyber sécurité
- Signer des protocoles Justice/Barreau/Intérieur sur ces problématiques de cybersécurité et cybercriminalité, et prévoir le partage d'informations entre chaque responsable



5. SIMPLIFIER LES PROCÉDURES D'ENQUÊTE SOUS PSEUDONYME DANS LE « DARKNET »

SYNTHÈSE DES RECOMMANDATIONS

À L'ATTENTION DES INSTANCES EUROPÉENNES



6. ADOPTER UN RÉGIME EUROPÉEN DE CONSERVATION DES DONNÉES

→ permettant de répondre aux besoins opérationnels des services répressifs et judiciaires: faciliter les enquêtes par la prise en compte de données conservées un an au plus

À L'ATTENTION DE L'ANSSI



7. INCITER LES ÉTATS SANCTUAIRES À METTRE FIN À L'IMPUNITÉ DES GROUPES CYBERCRIMINELS

→ Mettre un terme à l'installation confortable des grands groupes cybercriminels dans les pays sanctuaires en développant la solidarité entre les États pour obliger les États sanctuaires à prendre les mesures juridiques et économiques à cette fin



8. SIGNER DES PROTOCOLES AVEC L'ENSEMBLE DES AGENCES ET AUTORITÉS ADMINISTRATIVES INDÉPENDANTES CONCERNÉES

→ Inciter les agences et autorités administratives indépendantes à systématiser les procédures de signalement

À L'ATTENTION DES ENTREPRISES



9. INVESTIR DANS LA PRÉVENTION CONTRE LES CYBERATTQUES

→ Ces investissements doivent être humains (formation à la cyber sécurité), techniques (investissement dans des logiciels, outils de sauvegarde, audits, etc.), organisationnels (mise en place d'une cybergouvernance) et assurantiels



10. DÉPOSER IMMÉDIATEMENT PLAINTÉ EN CAS DE CYBERATTQUE

→ Condition nécessaire pour que les services mentionnés dans ce rapport soient saisis et puissent remonter et démanteler les réseaux

SOURCES

- (1) *2021 report: cyberwarfare in the C-suite, Cybersecurity ventures, janvier 2021*
- (2) *2021 report: cyberwarfare in the C-suite, Cybersecurity ventures, janvier 2021*
- (3) *2021 report: cyberwarfare in the C-suite, Cybersecurity ventures, janvier 2021*
- (4) Rapport du ministère de l'Intérieur, État de la menace numérique

MEMBRES DE LA COMMISSION

PRÉSIDENT

- **Bernard Spitz**, président du pôle International et Europe du MEDEF, ancien président de la Fédération française de l'assurance (FFA)

SECRÉTAIRE GÉNÉRALE

- **Valérie Lafarge-Sarkozy**, avocate associée, cabinet Altana

MEMBRES

- **Nicolas Arpagian**, VP Strategy & Public Affairs, Orange Cyberdefense
- **Brigitte Bouquot**, ancienne présidente de l'Association pour le management des risques et des assurances de l'entreprise (AMRAE), VP scientifique
- **Philippe Cotelte**, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space, Administrateur de l'AMRAE, président de la commission Systèmes d'information
- **Christophe Delcamp**, directeur adjoint des assurances de dommages et responsabilité, FFA
- **Émilie Dumérain**, déléguée juridique, Syntec Numérique
- **Agathe Lepage**, professeur, université Panthéon-Assas (Paris II)
- **Charles-Henry Madinier**, Director of Consulting Solutions, Marsh Advisory
- **Alexandre Menais**, Executive Vice President and Group Head of M&A, Strategy & Development, Atos
- **Séverine Oger**, chargée de mission / état-major de la sous-direction Opérations, ANSSI
- **Martin Pailhes**, responsable de l'équipe juridique « Information Technology – Intellectual Property », BNP Paribas
- **Christian Poyau**, président Micropole, président de la commission Transformation numérique du MEDEF
- **Myriam Quémener**, avocat général près la cour d'appel de Paris
- **Anne Souvira**, commissaire divisionnaire, chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du préfet de police de Paris
- **François Weil**, conseiller d'État
- **Leigh Wolfrom**, Policy analyst, Directorate for Financial and Enterprise Affairs, OCDE

ONT CONTRIBUÉ À LA RÉDACTION

- **Valérie Lafarge-Sarkozy**, avocate associée, cabinet Altana
- **Myriam Quémener**, avocat général près la cour d'appel de Paris
- **Anne Souvira**, commissaire divisionnaire, chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du préfet de police de Paris
- **Laetitia Daage**, avocate counsel, cabinet Altana

CONTACT PRESSE

GUILLAUME PRIGENT
guillaume.prigent@leclubdesjuristes.com
06 68 68 22 11

LE CLUB DES JURISTES
4, rue de la Planche 75007 Paris
www.leclubdesjuristes.com



RETROUVEZ-NOUS SUR     