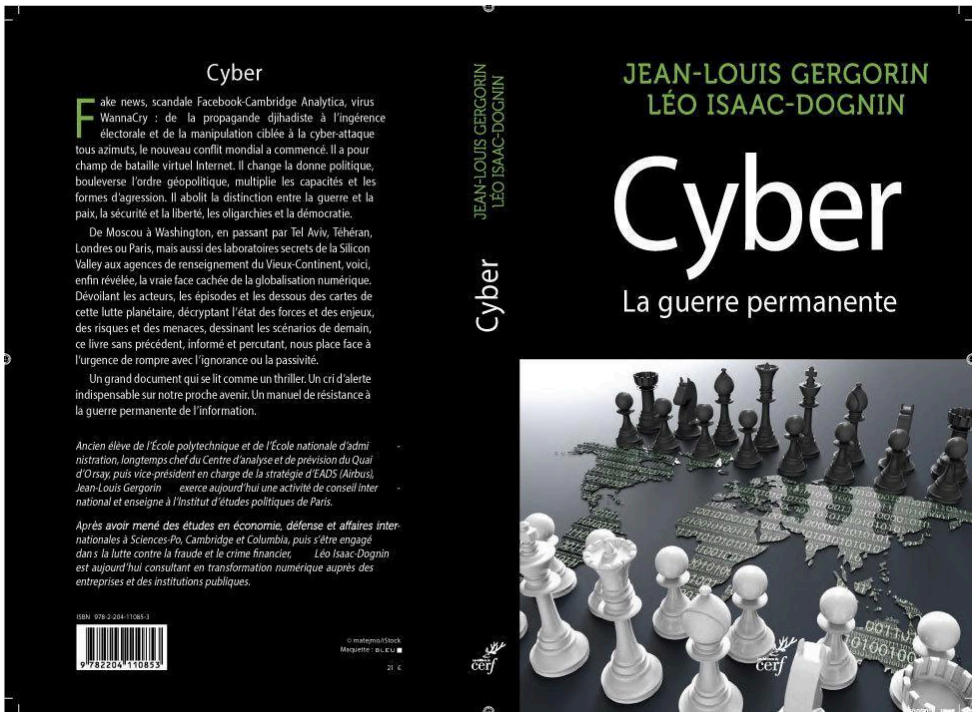
P1SD

Livre du Mois

Cyber, La guerre permanente, un ouvrage écrit par Jean-Louis Gergorin et Léo Isaac-Dognin



Première et quatrième de couverture de *Cyber, La guerre permanente* paru le 9 novembre 2018 (**Source** : LinkedIn de Jean-Louis Gergorin)

Auteur : Émilie Krezdorn

Le 24 février 2024

Introduction

Le Comité éditorial de l'association Panthéon-Sorbonne Sécurité-Défense (P1SD) vous propose un nouveau concept pour cette année 2024 : « Le Livre du Mois ». Chaque mois, les membres du comité vous feront découvrir un ouvrage sur nos thèmes de prédilection tels que la défense, la sécurité nationale et internationale, la stratégie militaire et l'armement.

En tant que rédactrice en chef du Comité éditorial, je suis honorée d'inaugurer ce nouveau concept avec *Cyber, La guerre permanente* écrit par Jean-Louis Gergorin et Léo Isaac-Dognin et publié aux éditions du Cerf en novembre 2018. L'objectif de cette production n'est pas de résumer l'ouvrage dans sa totalité mais plutôt de mettre en lumière les points saillants de l'argumentation pour, nous l'espérons, vous donner envie d'augmenter vos connaissances sur les notions connexes au « cyber », notamment sur la cyberguerre.

Nous commencerons par présenter les deux auteurs en se concentrant sur leurs parcours académiques et professionnels. Puis, nous analyserons le contexte d'écriture de l'ouvrage avant de présenter les grands moments de l'argumentation. Enfin, nous proposerons des pistes de réflexions sur les solutions apportées par les auteurs tout en vous partageant des travaux similaires.

I. Biographies

Jean-Louis Gergorin et Léo Isaac-Dognin ont des parcours académiques et professionnels variés. Leurs expériences respectives, qui leur ont permis de perfectionner leurs connaissances théoriques et empiriques dans le domaine cyber, ont été réinvesties dans l'écriture de cet ouvrage.

A. Jean-Louis Gergorin

Jean-Louis Gergorin, né le 22 avril 1946, est un ancien diplomate et homme d'affaires français, consultant en stratégie spécialiste des enjeux Cyber. Son parcours universitaire est riche : diplômé de la promotion 1966 de l'École Polytechnique puis de la promotion « Charles de Gaulle » de l'École Nationale d'Administration (ENA) en 1972 (remplacée en 2022 par l'Institut National du Service Public), il intègre le Stanford Executive Program en 1989.

Jean-Louis Gergorin rejoint ensuite le Ministère des Affaires étrangères à sa sortie de l'ENA et occupe dès 1973 le poste d'adjoint au chef de la planification stratégique pendant 5 ans avant de devenir le directeur de la planification stratégique jusqu'en 1984. En parallèle de ses fonctions, il est membre de la Commission franco-allemande permanente sur la sécurité et la défense. Puis, en septembre 1984, il intègre le groupe Matra où il occupe la position de directeur stratégique ainsi que de conseiller spécial de Jean-Luc Lagardère, président de Matra de 1977 à 2001. Matra est une entreprise française créée en 1941 et dissoute en 2003, spécialisée dans l'aéronautique, l'aérospatiale, l'automobile, les télécommunications et la défense. L'acronyme de « **M**écanique **A**viation **Tra**ction », ses actions s'étendent progressivement aux métiers de l'horlogerie, de la presse, des médias ainsi que des divertissements sous l'impulsion de Lagardère.

Jean-Louis Gergorin est également connu pour ses différentes fonctions occupées au sein du Conseil d'État : auditeur de 1972 à 1976, il est ensuite auditeur en détachement, maître des requêtes en détachement et enfin maître des requêtes en disponibilité. Finalement, Jean-Louis Gergorin restera ainsi près de 28 ans au Conseil d'État. Pour autant, cela est loin d'égaler ses 47 ans comme maître de conférence à la Paris School of International Affairs de Sciences Po Paris (PSIA). Il fait aussi partie des enseignants qui réintroduisent l'étude de la géopolitique au sein de l'établissement et depuis 2017, présente un cours intitulé « le nouveau bouleversement stratégique », basé sur ses thèmes de prédilections.

En juillet 2000, Jean-Louis Gergorin devient directeur de la coordination stratégique et membre du comité exécutif chez EADS ou European Aeronautic Defence and Space company, plus communément appelé sous le nom d'Airbus. Proche des services de renseignements français, il est chargé de la sécurité des activités économiques d'EADS et impulse la stratégie qui permet à l'entreprise de rivaliser avec Boeing dans l'équipement de l'US Air Force en avions ravitailleurs. En 2004, suite aux tensions nées de la guerre en Irak, il organise avec le Center for Strategic and International Studies (CSIS) une rencontre entre diplomates français et américains de haut niveau. En 2011, le classement Global go-to Think Tanks nomme d'ailleurs, pour la cinquième année consécutive, le CSIS comme étant le meilleur cercle de réflexion en matière de sécurité et affaires internationales.

Par ailleurs, le 26 avril 2007, Jean-Louis Gergorin fonde la société JLG Strategy, qui a pour mission le conseil en stratégie aérospatiale, défense et cyber, pour les comités proposant des actions politiques mais aussi les ONG. La même année, il publie un ouvrage intitulé

Rapacités expliquant son implication dans l'affaire Clearstream (2001-11) et son désir de protéger l'entreprise EADS des malversations financières souterraines. Il s'agit d'une affaire de blanchiment d'argent qui met en cause les milieux politico-financiers *via* une banque basée au Luxembourg. Le journaliste Denis Robert avait révélé l'affaire qui fera scandale dans son ouvrage intitulé *Révélations* publié en 2001. À partir de 2004, un règlement de compte au sommet de l'État envahit l'espace judiciaire, politique et médiatique. *Rapacités* donne à l'auteur l'occasion de décrire une partie de sa carrière ainsi que les jeux économico-financiers occultes qui ont cours chaque jour dans le monde. Jean-Louis Gergorin publiera également deux autres ouvrages dont *Cyber : la guerre permanente* en 2018 suivi de *Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ?* en 2020, co-écrits avec Léo Isaac Dognin. La même année, Jean-Louis Gergorin cosigne trois tribunes dans le journal *Le Monde*, avec Bernard Barbier, ancien directeur technique de la DGSE, et l'amiral Édouard Guillaud, ancien chef d'état-major des armées, sur l'importance actuelle et surtout future des enjeux cyber, à savoir le besoin impérieux d'une stratégie nationale en la matière, la nécessité de mettre en œuvre le concept de cybercoercition dans une logique de dissuasion et enfin l'impréparation européenne en la matière au moment de l'affaire Pegasus.

B. Léo Isaac-Dognin

Léo Isaac-Dognin est quant à lui un jeune titulaire d'un Bachelor of Arts de l'Université de Cambridge, obtenu en 2012. Il s'engage en 2015 dans le Master en Affaires Internationales de Sciences Po Paris où il se spécialise dans les domaines de la sécurité, de la cybersécurité et du management aérospatial. En parallèle, il obtient en 2017 un Master d'Administration Publique (MPA en anglais) de l'Université de Columbia, avec pour majeure le management de l'économie de l'information et les politiques relatives à la technologie.

En septembre 2012, Léo Isaac-Dognin intègre la Financial Conduct Authority, une instance de régulation du secteur financier britannique, indépendante du gouvernement qui veille à l'application du droit boursier britannique. Ayant d'abord occupé le poste d'analyste légiste spécialisé dans la fraude et le renseignement financier, il devient analyste politique avant d'être nommé conseiller spécial des membres du comité exécutif. Un temps consultant en 2017 pour Capgemini Invent, il prend la tête du groupe en juillet 2020. Capgemini Invent est considéré comme l'un des partenaires stratégiques des plus grandes organisations mondiales. Déployé dans plus de 50 pays et réalisant un chiffre d'affaires de près de 22

milliards d'euros, le groupe a pour objectif d'engager la transition technologique des entreprises en utilisant l'intelligence artificielle générative. Le groupe utilise notamment le cloud, la data, l'IA, la connectivité des logiciels, l'ingénierie digitale ainsi que d'autres plateformes numériques pour aider les entreprises et répondre à leur besoin en stratégie, design et management.

Depuis janvier 2019, Léo Isaac-Dognin est également maître de conférence à Sciences Po Paris où il dispense le cours "IA in the Public Sector" dans le cadre du Master Politiques Publiques, en collaboration avec Sonia Gorjup, directrice du Citizen Services chez Capgemini Invent et d'Étienne Grass, directeur exécutif chez Capgemini Invent France. En parallèle de ses fonctions professorales, il est un Engagement Manager chez McKinsey & Company depuis mars 2022. Sa mission principale est de guider l'action collective au service d'un projet client et ses produits finaux. Il est chargé d'analyser la marché dans lequel le projet sera intégré, de la conception à la mise en œuvre des approches de performance commerciale, en développant des solutions sur mesure et en travaillant en étroite collaboration avec les clients. Il s'agit principalement de collecter et d'analyser l'information, de formuler et tester les hypothèses ainsi que d'élaborer des recommandations qui seront présentées à la direction de l'entreprise cliente.

II. Contexte d'écriture

Le contexte d'écriture est essentiel pour comprendre la thèse de Jean-Louis Gergorin et Léo Isaac-Dognin. En effet, en 2018, date de publication de *Cyber, La guerre permanente*, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est l'autorité nationale en matière de cybersécurité et de cyberdéfense, publie son rapport d'activité pour l'année 2017 et évoque « un tournant pour la sécurité numérique en France ». Si l'année 2016 est marquée par « une prise de conscience », nous nous concentrerons principalement sur les éléments présentés dans le rapport de 2017 qui dresse les enjeux en matière de cybersécurité.

A. Un « Cyber panorama » de l'année 2017

1. Le 3 avril 2017 - **ATTAQUE : APT10** : Publication d'un rapport faisant état d'une campagne d'espionnage de grande ampleur dont le mode opératoire dénommé APT10 (également connu sous le nom de Red Apollo, un groupe de cyberespionnage parrainé

par l'État chinois qui opère depuis 2006) repose sur la compromission des fournisseurs et sous-traitants des entreprises ciblées pour les atteindre ;

2. Le 8 et 14 avril 2017 - **MENACE : Shadow Brokers** : Le groupe Shadow Brokers publie gratuitement en ligne une liste de plusieurs outils informatiques offensifs et très sophistiqués porteurs de vulnérabilités de type O Day. Également connu sous la terminologie de faille zero-day, il s'agit de toute vulnérabilité d'un logiciel ou d'un système d'exploitation pour lequel aucun correctif n'a encore été publié. Ces failles sont des cibles de choix pour les hackers, dans la mesure où elles offrent l'opportunité d'accéder facilement aux ordinateurs et données. Dans cette catégorie, nous retrouvons Eternal Blue sur lequel se sont appuyées les deux campagnes d'attaques WannaCry et NotPetya ;

3. Année 2016 - **ATTAQUE : Parti démocrate USA** : Perturbation des élections présidentielles américaines *via* la publication de milliers d'e-mails des responsables démocrates avec des leaks ciblés sur la candidate démocrate Hillary Clinton. Ces attaques semblent être attribuées aux services de renseignements russes, par l'intermédiaire de Fancy Bear, dont les liens avec le gouvernement n'ont jamais été confirmé ;

4. Le 5 mai 2017 - **MENACE : Présidentielles françaises** : Suite à l'observation et à l'analyse de la campagne de déstabilisation des élections américaines, la France active un plan d'action pour grâce aux efforts de ses services de renseignements pour éviter toute ingérence étrangère ;

5. Du 13 mai au 30 juillet 2017 - **ATTAQUE : Equifax** : Série d'attaques exploitant une faille d'un serveur Web de l'agence d'évaluation de crédit Equifax, conduisant au vol de bases de données contenant les informations à caractère personnel de plus de 145 millions d'Américains ;

6. Décembre 2017 - **MENACE : 4IQ Leaks** : L'entreprise 4IQ, spécialisée dans la recherche de données personnelles publiées sur Internet, diffuse un article relatif à la découverte, sur le darknet, d'une base de données libre d'accès recensant près d'1,4 milliard d'identifiants et mots de passe, etc.

B. Les enseignements de l'année 2017 retenus par l'ANSSI

Guillaume Poupard, directeur général de l'ANSSI de 2014 à fin 2022, a déclaré que l'année 2017 était une année électorale d'importance, avec plusieurs scrutins nationaux aux enjeux de cybersécurité majeurs. Cette année a également permis à l'ANSSI de mieux faire comprendre que le risque cyber n'est pas – n'est plus pour certains attentistes – l'affaire des autres ou un dossier à traiter « plus tard », mais bel et bien un enjeu actuel et prégnant. Guillaume Poupard a enfin expliqué que les attaques qui ont émaillé le calendrier national adoptent une dimension nouvelle. Les cyberattaques sont en effet plus sophistiquées, mieux élaborées, plus destructrices et touchent désormais l'ensemble de la société, du citoyen à la grande entreprise et s'attaquent même aux fondements de la démocratie française.

On assiste en outre à un travail de coopération avec les États membres de l'Union Européenne à travers l'élaboration puis la transposition de la directive Network and Information Security (NIS), structurée autour de 4 axes dans le droit national français et adoptée dès juillet 2016. Tout d'abord, elle prévoit le renforcement des capacités nationales de cybersécurité. Les États membres doivent « se doter d'autorités nationales compétentes en matière de cybersécurité, d'équipes nationales de réponse aux incidents informatiques (CSIRT) et de stratégies nationales de cybersécurité ». En France, ces fonctions sont respectivement endossées par l'ANSSI, le CERT-FR et la stratégie nationale pour la sécurité du numérique. Puis, la directive entend établir « un cadre de coopération volontaire entre Etats membres de l'UE » par la création de « groupe de coopération » ainsi qu'un « réseau européen des CSIRT » des États membres visant à faciliter le partage d'informations techniques sur les risques et les vulnérabilités. Le troisième axe de la directive se concentre sur le renforcement de la cybersécurité « d'opérateurs de services essentiels au fonctionnement de l'économie et de la société » *via* la définition de règles nationales sur la cybersécurité et « l'obligation pour les opérateurs de notifier les incidents ayant un impact sur la continuité de leurs services essentiels ». Enfin, la direction prévoit « l'instauration de règles européennes communes en matière de cybersécurité » par des prestataires de services numériques notamment.

Le constat est clair : les tentatives de déstabilisation sont de plus en plus complexes, sophistiquées et nombreuses. L'année 2017 marque un tournant dans la conduite des cyberattaques par leur intensité, leur caractère inédit et surtout par les nouvelles craintes

qu'elles font peser. En 2018, 5 grandes tendances ont été observées en France et en Europe par l'ANSSI, dans son rapport publié en 2019 : 1) l'exfiltration des données stratégiques, 2) la conduite d'attaques indirectes mais aussi 3) d'opérations de déstabilisation ou d'influence, 4) la génération de cryptomonnaies, et enfin, 5) la fraude en ligne. Par conséquent, les préoccupations autour de la cybersécurité sont devenues centrales dans la géopolitique mondiale actuelle, les cyberattaques étant de puissants déstabilisateurs de la sécurité internationale. Les activités cybernétiques, y compris les tentatives présumées d'ingérence russe dans les élections américaines de 2016, sont devenues des enjeux de politique étrangère majeurs. Les grandes puissances, tout comme les acteurs privés, cherchent à construire et à imposer des normes de comportement dans le cyberespace aux frontières sans cesse redéfinies, tandis que les cybermenaces, de plus en plus sophistiquées, ciblent les infrastructures critiques à l'échelle mondiale.

III. La thèse de Jean-Louis Gergorin et Léo Isaac-Dognin

En novembre 2018, Léo Isaac-Dognin et Jean-Louis Gergorin publient *Cyber, La guerre permanente*, proposant une analyse géopolitique des principaux incidents cyber depuis le début des années 2000 et des enjeux qui en découlent. L'ouvrage sera d'ailleurs largement encensé par la presse lors de sa sortie.

Le terme « cyber » est souvent associé aux domaines de la technologie, de la sécurité informatique et de la guerre dans le cyberespace. Il englobe une gamme d'activités, de menaces et de concepts liés à l'utilisation des systèmes informatiques et des réseaux fortement reliés au développement de la data science ainsi que de l'IA. Les auteurs abordent les différents concepts liés au cyber, notamment celui du cyberspace qui désigne l'environnement virtuel créé par les systèmes informatiques interconnectés, par exemple l'Internet, où les interactions et les transactions électroniques ont lieu. Ce cyberespace appelle à définir une autre notion portant sur la protection des données et des relations, synthétisé par la notion de cybersécurité désignant la protection des systèmes informatiques, des réseaux et des données contre les cybermenaces telles que les attaques informatiques, les piratages, les logiciels malveillants et d'autres formes d'activités malveillantes dans le cyberespace. Finalement, la cybersécurité assure la protection du cyberespace menacée en permanence par le cybercrime ou activité criminelle de type cyber comme le vol d'identité en ligne, la fraude par carte de crédit, la diffusion de logiciels malveillants, la cyber-extorsion, etc. Les auteurs font état

d’une cyberguerre définit en introduction comme « l’utilisation des moyens numériques à des fins de contrôle ». Jean-Louis Gergorin et Léo Isaac-Dognin affirment qu’il s’agit d'une nouvelle forme majeure d’action stratégique qui transcende les diverses conceptions de la guerre [dite traditionnelle] et engage ainsi des acteurs divers provoquant des dommages technologiques importants.

Les auteurs ont fait le choix d’une argumentation thématique et historique : à travers une chronologie relativement progressive des différentes affaires de cybercriminalité et de cybersécurité qui ont traversé ces vingt dernières années, les auteurs définissent et détaillent les différents concepts clés du « cyber ». La thèse de Jean-Louis Gergorin et Léo Isaac-Dognin repose ainsi sur une analyse approfondie de la nature, des défis et des implications de la cyberguerre dans un contexte géopolitique contemporain aux frontières sans cesse remodelées.

Leur thèse, dont la pierre angulaire repose sur la mise en garde contre les dangers de la cybercriminalité qui conduisent à une situation de « guerre permanente », est détaillée en 7 chapitres et comprend une logique graduelle en 4 étapes.

Tout d’abord, les auteurs introduisent le concept de cyberguerre en définissant ses contours et en mettant en évidence sa singularité par rapport aux formes traditionnelles de conflits. Ils présentent l'idée selon laquelle la cyberguerre est devenue une réalité incontournable dans le paysage géopolitique moderne en raison de la dépendance croissante des sociétés aux technologies de l'information et de la communication.

Puis, ils analysent la nature de la cyberguerre. Asymétrique, puissante et déstabilisatrice, elle engage des acteurs divers tels que des États, des associations terroristes mais aussi des individus isolés qui utilisent de nombreuses armes, véritables outils de puissance dans les conflits internationaux.

Leur argumentation se poursuit sur l’étude des défis et des enjeux sécuritaires. Prenant exemples sur les grandes puissances contemporaines que sont les États-Unis, la Chine, la Russie et l’Europe, les auteurs questionnent la cyberguerre dans une perspective de sécurité nationale et internationale. Cela inclut la vulnérabilité des infrastructures critiques, la protection des données sensibles et les implications pour la souveraineté des États. A travers les nombreuses affaires de cybercriminalité, les auteurs soulignent également les préoccupations croissantes concernant la vie privée des individus, la protection des données personnelles et les risques pour la sécurité des citoyens ordinaires.

Enfin, Jean-Louis Gergorin et Léo Isaac-Dognin concluent en appelant à une réponse proactive et coordonnée face à la menace de la cyberguerre. Ils insistent sur l'importance de la coopération internationale dans le développement de politiques et de stratégies de défense efficaces. Ils proposent même des recommandations fondées sur quatre scénarios possibles à la fin de leur ouvrage afin de renforcer la cybersécurité des États, des organisations et des individus, ainsi que pour promouvoir la stabilité et la sécurité dans le cyberespace.

Finalement, il est possible de retenir cinq points saillants de la thèse de Jean-Louis Gergorin et Léo Isaac-Dognin :

1. La cyberguerre est une réalité contemporaine incontournable dans le paysage géopolitique international qui a intégré le cyberespace.
2. La cyberguerre est asymétrique car même les petits acteurs ou cybercriminels isolés peuvent causer des dommages considérables à des entités étatiques ou des grandes entreprises internationales.
3. La cyberguerre est une menace qui s'établit à tous les niveaux de la société, ce qui implique une réponse adaptée et personnalisée.
4. La coopération internationale est essentielle pour lutter efficacement contre les problèmes posés par la cyberguerre. La communauté internationale doit, malgré les difficultés culturelles et les orientations politiques internes affiliées au thème du cyber, arriver à construire des politiques pour identifier, prévenir et lutter contre les attaques cyber.
5. La cyberguerre engage directement la sécurité des individus, de leurs informations personnelles ainsi que de leur vie privée.

IV. Pistes de réflexion et ouvrages connexes

À titre personnel, j'ai beaucoup apprécié la lecture de cet ouvrage. Complet et dynamique, il nous présente de façon concise les notions connexes au concept « cyber ». Les définitions données, alliées aux multiples exemples, font de ce livre une véritable mine d'or d'informations ainsi qu'une très belle entrée en matière pour les novices en cybersécurité.

Nous pouvons toutefois soulever deux points d'amélioration. Tout d'abord, si l'ouvrage est construit comme une véritable leçon historique qui se lit comme un thriller,

mélangeant intrigue et suspens, et qu'il permet de comprendre aisément les différentes méthodes utilisées au cours d'une cyberattaque, les exemples proposés font parfois « effet catalogue ». L'ouvrage aurait donc pu gagner en efficacité en étant plus synthétique dans ses choix d'exemples qui peuvent surcharger l'argumentation. La seconde piste que les auteurs auraient pu envisager est la mobilisation de solutions techniques concrètes. En effet, ils se focalisent plus sur des solutions politiques, qui sont d'ailleurs extrêmement difficiles à mettre en place selon ces derniers, plutôt que sur des solutions concrètes. Jean-Louis Gergorin et Léo Isaac-Dognin auraient donc pu s'appuyer davantage sur leurs expériences et compétences professionnelles pour présenter des solutions techniques innovantes. Ces deux aspects auraient pu contribuer à une lecture plus fluide ainsi qu'à une compréhension plus précise de la cyberguerre, ses problématiques et ses enjeux.

En résumé, *Cyber, La guerre permanente* met en lumière l'importance croissante de la cyberguerre ainsi que ses menaces complexes et évolutives. Jean-Louis Gergorin et Léo Isaac-Dognin insistent sur la nécessité d'une réponse globale et d'une coopération de long terme pour espérer endiguer le fléau de la cybercriminalité et relever les défis sécuritaires nationaux et internationaux.

Si vous souhaitez développer vos connaissances en cybersécurité, je vous recommande également les ouvrages suivants : *Cybersécurité et Cyberdéfense : Enjeux Stratégiques* de Yann Salamon publié en 2020 ainsi que *Counterstrike, The Untold Story of America's Secret Campaign Against Al Qaeda* d'Eric Schmitt et Thom Shanker publié en 2011.

Bibliographie

Pour en apprendre davantage sur les auteurs de *Cyber, La guerre permanente* voir les pages linkedIn des auteurs Jean-Louis Gergorin (ainsi que sa page wikipedia) et Léo Isaac Dognin

Sur l'affaire Clearstream, écoutez le podcast de France inter (53 min) « Affaire Clearstream : règlement de comptes au sommet de l'État » du 23 mai 2017, disponible en ligne https://www.radiofrance.fr/franceinter/podcasts/affaires-sensibles/affaire-clearstream-reglement-de-comptes-au-sommet-de-l-etat-7841980 [consulté le 01 mars 2024]

Retrouvez les rapports d'activités annuels de l'ANSSI https://cyber.gouv.fr/rapports-dactivites et la présentation de la directive européenne sur le Network and Information Security (NIS) https://cyber.gouv.fr/actualites/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la [consultés le 01 mars 2024]