MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

Direction générale du Trésor

Horizon ASEAN

Lettre d'information économique

Une publication du SER de Singapour – N°44 (mai 2024)

SOMMAIRE

Crédit photo : Unsplash.

Cybersécurité en Asie du Sud-Est : un « far-east » numérique ?

Propulsée par la transformation technologique des pays de la région, l'économie numérique progresse rapidement en Asie du Sud-Est, avec un volume d'affaires qui pourrait atteindre jusqu'à 1 000 Mds USD d'ici 2030, faisant de cette région le marché internet à la croissance la plus rapide au monde. Parallèlement, cette croissance s'accompagne d'une hausse significative des cyberattaques dans la région, en augmentation de 45% pour celles visant les entreprises entre 2021 et 2022. Alors que les pays de l'ASEAN doivent faire face à une série de défis complexes et multiformes dans la lutte contre ces cybermenaces, un champ d'opportunités économiques et de développement pourrait s'ouvrir pour la France et ses entreprises dans la région.

La transformation technologique de l'ASEAN et les tensions géopolitiques dans la région entraînent une hausse de la cybercriminalité

Avec un nombre de cyberattaques en hausse, le risque économique pour les entreprises de la zone est majeur. En 2022, Singapour a enregistré une multiplication par quatre du nombre de cyberattaques contre ses entreprises par rapport à l'année précédente, passant de 207 000 à 890 000 incidents relevés par la société de cybersécurité Kaspersky. D'autres pays, comme la Malaisie (+197%), la Thaïlande (+63%), l'Indonésie (+46%) et les Philippines (+29%), ont également été confrontés à une croissance significative des cyberattaques. Seul le Vietnam a connu une légère baisse (-12%) après avoir enregistré 2.5 millions d'incidents en 2022 contre 2.8 millions en 2021. Poursuivant cette tendance, l'année 2023 a enregistré un nombre record de victimes de cyber-extorsion, avec une augmentation de 67% en Asie du Sud-Est en glissement annuel (g.a.), contre une hausse de 46% à l'échelle mondiale[1]. En 2022, les trois quarts des entreprises en Malaisie et aux Philippines avaient été victimes de cyberattaques et la moitié des entreprises à Singapour et en Indonésie[2]. Pour les entreprises, les logiciels malveillants (« malware ») figuraient en tête des causes principales de cyberattaques en Indonésie (35% des attaques), aux Philippines (29%) et en Malaisie (21%) tandis que les attaques par déni de service (« DDoS ») constituaient le modus operandi privilégié des cybercriminels à Singapour (22%). Au T4 2023, la cité-Etat était la principale cible des attaques DDoS HTTP (où les assaillants ciblent les serveurs web en envoyant un trafic HTTP excessif pour les submerger, rendant ainsi le service inaccessible aux utilisateurs légitimes) dans le monde, devant les Etats-Unis et le Canada. En Malaisie, 57% des cyberattaques ont entraîné des vols de données (« data breach »), tandis qu'en Indonésie, 62% des entreprises ont signalé des interruptions d'activités à la suite de cyberattaques. Près d'un quart des cyberattaques aux Philippines et en Indonésie a entraîné une demande de rançon. En 2023, le coût moyen d'un vol de données en Asie du Sud-Est a atteint pour la première fois 3 M USD[3], +6% en g.a., dépassant celui de l'Australie (2,7 M USD) et de l'Inde (2,18 M USD). Parmi les secteurs les plus touchés, la finance et l'énergie enregistrent les coûts les plus élevés, respectivement de 4,81 M USD et 3,60 M par extorsion en moyenne.

Le cyberespace est un nouveau vecteur d'ingérence étatique à des fins d'espionnage et de déstabilisation. Au cœur des tensions géopolitiques entre la Chine et les Etats-Unis, les pays de l'ASEAN sont la cible de cybercriminels parrainés par l'État. Le cyberespace est devenu un champ d'action privilégié pour les services de renseignement étrangers, qui l'utilisent directement ou indirectement via des intermédiaires, afin de promouvoir leurs agendas stratégiques. Sur 86 campagnes de menaces persistantes avancées (attaques informatiques sophistiquées et continues qui s'infiltrent furtivement dans les systèmes informatiques d'une organisation pour accéder à des informations sensibles, voler des données ou perturber les opérations ; « APT ») observées par Cyfirma[4], une société de cybersécurité singapourienne, de janvier à août 2023, 68 visaient l'Asie du Sud-Est, soit près de 80% d'entre elles. Ces « APT » étaient principalement dirigées vers Singapour, suivi de la Thaïlande, du Vietnam et de l'Indonésie, et visaient à la fois des administrations et des infrastructures critiques.

Les « APT » en Asie du Sud-Est

ASEAN – En amont d'un sommet entre les Etats-Unis et l'ASEAN en 2022, des cybercriminels auraient dérobé des correspondances d'e-mails du Secrétariat de l'ASEAN et des contacts dans les États membres[5]. Plusieurs attaques de nature similaire ont été enregistrées depuis 2019.

Philippines – En août 2023, l'APT chinois Stately Taurus est accusé d'avoir compromis une agence gouvernementale philippine, quelques jours après qu'un navire de la Garde côtière chinoise a tiré avec son canon à eau sur un navire philippin.

Chine et Vietnam – En 2020, l'APT vietnamien OceanLotus a ciblé le ministère chinois de la Gestion des Urgences et le gouvernement municipal de Wuhan pour obtenir des informations sur la pandémie de COVID-19. En 2021, OceanLotus est également accusé d'avoir lancé plusieurs attaques par logiciels espions contre des militants des droits humains vietnamiens. En 2019, il avait déjà ciblé les constructeurs automobile BMW, Hyundai et Toyota.

La vulnérabilité des infrastructures critiques dans la région fait peser un risque mondial. En 2023, les infrastructures critiques mondiales (équipements médicaux, électriques, de communication, de traitement des déchets, de fabrication et de transport) ont subi 420 millions de cyberattaques, soit 13 attaques chaque seconde[6]. L'augmentation des cyberattaques menace les secteurs économiques vitaux des pays de l'ASEAN, qui deviennent plus vulnérables à mesure que la transformation numérique se poursuit dans la région. En Asie, ces attaques ciblent principalement les agences gouvernementales (22% du total des attaques contre des organisations), les entreprises industrielles (9%), les entreprises informatiques (8%) et les institutions financières (7%)[7].

Cyberattaques et fuites de données visant des organisations en ASEAN

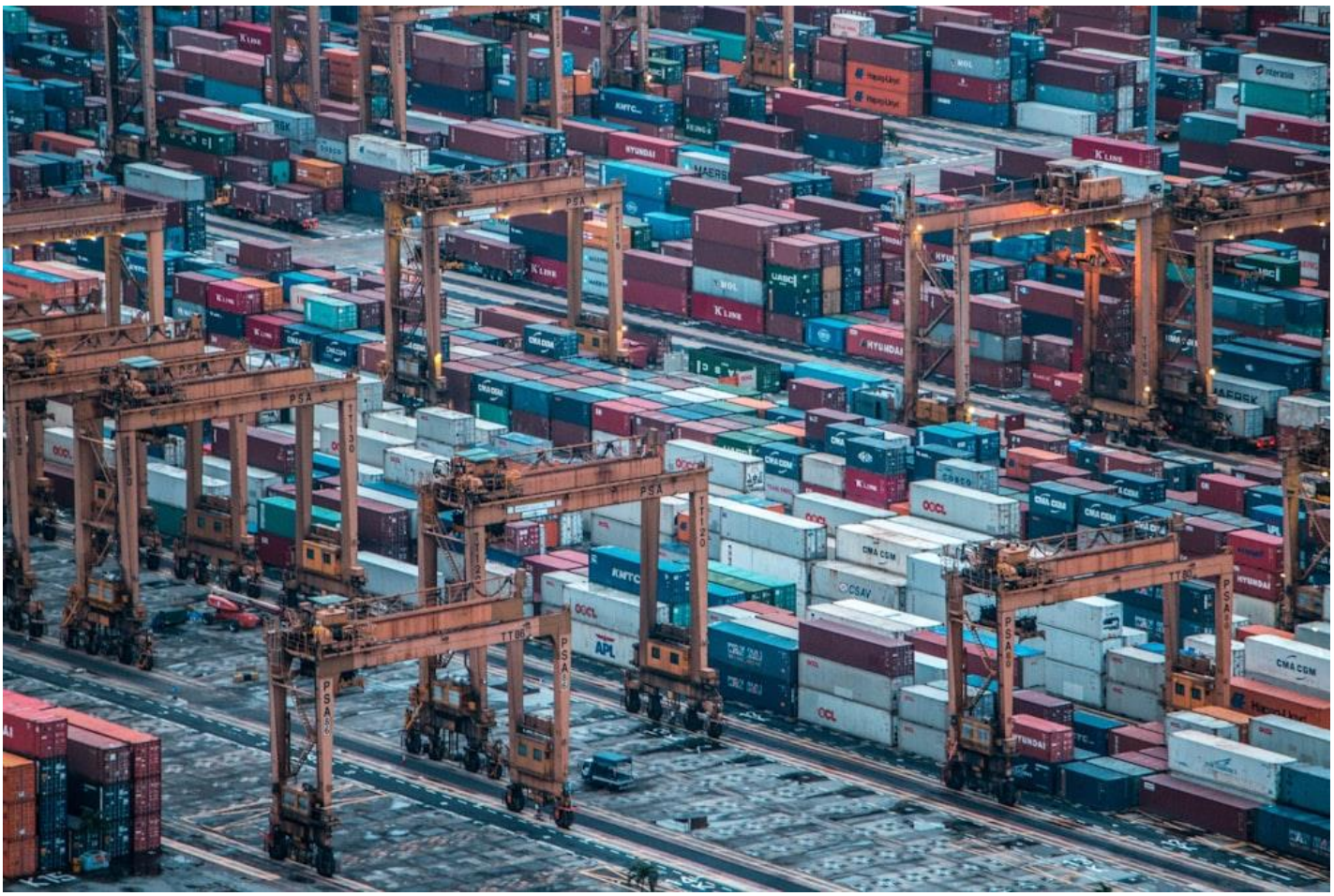
Direction générale de l'immigration, Indonésie, juillet 2023 – Les données de plus de 34 millions de détenteurs de passeports indonésiens, stockées par la Direction générale de l'immigration, ont été piratées et mises en vente pour 10 000 USD.

Bank Syariah Indonesia (BSI), Indonésie, mai 2023 – La plus importante banque islamique d'Indonésie a subi une cyberattaque majeure, entraînant la fuite d'informations 15 millions de comptes-clients, après que les négociations pour le paiement de la rançon ont échoué. Les données compromises incluaient notamment les noms des détenteurs de compte, leurs numéros de compte, les soldes actuels et l'ensemble de leurs historiques de transactions.

Philippines, avril 2023 – Une fuite de données sur un portail de recrutement en ligne non-sécurisé a exposé plus d'un million de dossiers de candidats et d'employés de plusieurs agences gouvernementales, dont la Police nationale Philippine (PNP), le Bureau national d'enquête (NBI) et le Bureau des impôts internes (BIR).

SingHealth, Singapour, 2018 – Lors d'une cyberattaque à Singapour, des pirates ont accédé aux bases de données de SingHealth, le plus grand groupe de santé dans le pays, volant les données personnelles de 1,5 million de patients, y compris les feuilles de soins du Premier ministre Lee Hsien Loong et d'autres membres du gouvernement.

En 2018, une simulation[8] estimait qu'une cyberattaque ciblant six ports majeurs au Japon, en Malaisie et à Singapour pouvait engendrer des pertes économiques mondiales allant jusqu'à 41 Mds USD. Si l'attaque s'étendait aux 15 principaux ports de la région Asie-Pacifique, ces pertes pourraient s'élever jusqu'à 110 Mds USD. En plus des conséquences sur l'économie mondiale, une perturbation de la chaîne d'approvisionnement dans la région aurait des répercussions catastrophiques, non seulement sur l'économie singapourienne (où le secteur maritime représente 7% du PIB), mais aussi sur l'économie régionale dans son ensemble (le secteur maritime contribue autour de 40% au PIB malaisien[9]).



Port de Singapour. Crédit photo : Unsplash.

Des défis complexes et multiformes dans la lutte contre les cybermenaces pour les pays de l'ASEAN et une réponse régionale en cours de définition

De la Birmanie à Singapour, le degré de préparation contre les cyberattaques varie considérablement d'un pays à l'autre. Pays mature sur les sujets de cybersécurité, Singapour a établi son Agence de cybersécurité (CSA) en 2015, a adopté une Loi sur la cybersécurité en 2018 (modifiée en 2024), a révisé sa stratégie nationale dans le domaine en 2021, et organise chaque année l'évènement-phare de la cybersécurité dans la région, la Semaine Internationale de la Cybersécurité, auquel a dernièrement participé le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Vincent Strubel. Plus récemment, en février 2023, Singapour a acté dans son budget pour 2024, la création d'un nouveau Centre de commandement de cybersécurité national, pour mieux coordonner les opérations de défense cyber de Singapour, améliorer la collaboration entre l'industrie et le monde universitaire, et stimuler l'innovation en matière de cybersécurité. La Malaisie de son côté a développé une stratégie de cybersécurité, créé son Agence nationale en 2017, et vient d'adopter une Loi sur la cybersécurité en avril 2024. La Thaïlande, dans le cadre de son plan « Thailand 4.0 », a introduit des lois sur la protection des données et la cybersécurité en 2019. Les Philippines ont adopté une loi sur la protection des données en 2012 et prévoient un nouveau plan de cybersécurité pour 2023-2028. L'Indonésie, sans législation spécifique en cybersécurité, se repose sur un règlement de 2019, avec une loi sur la protection des données en 2022 et une stratégie nationale en 2023. Le Vietnam a renforcé sa législation en 2019 et lancé une stratégie nationale en 2022. Le Brunei a mis en place une nouvelle loi en 2023. En revanche, le Cambodge, le Laos et la Birmanie restent limités en ressources et en infrastructure.

FOCUS

La réponse réglementaire en ASEAN

Singapour a établi son Agence de cybersécurité (CSA) en 2015 et promulgué des lois clés, dont sa première Loi sur la cybercriminalité dès 1993 (amendée en 2023), suivie de la Loi sur la protection des données personnelles en 2013 puis de la Loi sur la cybersécurité en 2018. Depuis 2016, le pays dispose d'une stratégie nationale de cybersécurité, la dernière datant de 2021. Singapour est également l'hôte d'une importante conférence professionnelle en cybersécurité, la Semaine Internationale de la Cybersécurité de Singapour (SICW), organisée par la CSA.

En Malaisie, bien que le gouvernement ait élaboré une Stratégie de cybersécurité (MCSS) pour la période 2020-2024 et établi son Agence nationale de cybersécurité (NACSA) en 2017, le pays ne disposait jusqu'alors d'aucune législation unifiée et spécialisée dans le domaine de la cybersécurité. En avril 2024, un projet de Loi sur la cybersécurité a été adopté pour compléter la législation existante.

Dans la continuité du projet « Thailand 4.0 », Bangkok a mis en œuvre la Loi sur la protection des données personnelles en 2019 (avec une mise en conformité en 2022) ainsi que la première Loi sur la cybersécurité la même année, un texte controversé (il autorise les autorités administratives à « exercer un contrôle sur Internet » de manière illimitée et à arrêter tout utilisateur sans avoir besoin de recourir à une autorité judiciaire, en cas de « situation d'urgence en cybersécurité »), dont la mise en œuvre est gérée par l'Agence nationale de cybersécurité (NCSA).

Dans le cadre de leur Politique nationale de sécurité pour 2011-2016, les Philippines ont adopté en 2012 une Loi sur la protection des données personnelles et ont amélioré leur cadre de cybersécurité grâce à la Loi sur la prévention de la cybercriminalité la même année. Le pays s'est doté d'un nouveau Plan national de cybersécurité (NCSP) pour 2023-2028, qui encourage la création d'une Loi sur la cybersécurité.

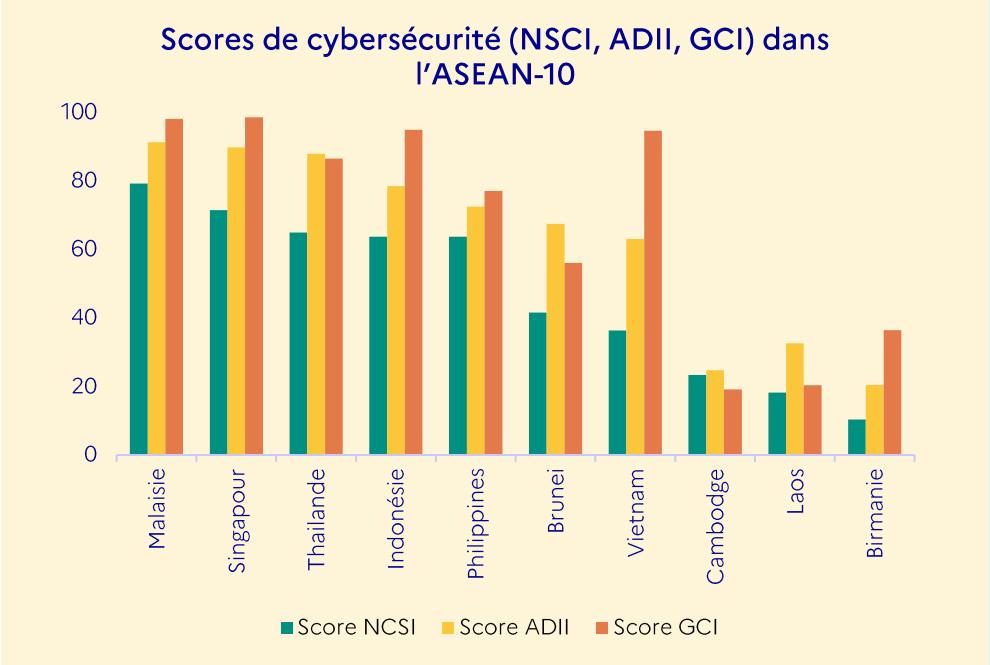
L'Indonésie ne possède actuellement pas de législation spécifique en matière de cybersécurité. Les dispositions relatives à la cybersécurité sont principalement couvertes par le Règlement sur la fourniture de systèmes et de transactions électroniques de 2019 qui régit les activités des opérateurs électroniques, généralement définis comme toute personne, administration, entité commerciale. Le pays s'est également doté d'une Loi sur la protection des données personnelles en 2022, et de sa première Stratégie nationale de cybersécurité et gestion des risques cyber en 2023.

Le Vietnam a progressivement renforcé ses efforts en matière de cybersécurité et introduit une Loi sur la cybersécurité en 2019, qui oblige notamment certains acteurs économiques opérant dans dix secteurs régulés à localiser le stockage et le traitement des données sur le territoire national. Particulièrement touché par les cyberattaques, le pays a lancé en 2022 sa Stratégie nationale de cybersécurité et de sûreté pour 2025-2030, qui encourage le développement de politiques publiques et de lois en matière de cybersécurité, l'amélioration des capacités en cybersécurité, et encourage également les infrastructures critiques vietnamiennes à se fournir auprès d'entreprises vietnamiennes. Le pays développe déjà ses propres infrastructures 5G avec l'opérateur Viettel, lié à l'armée.

Après avoir adopté une Loi spécifique sur la cybercriminalité en 2007, le Brunei vient de se doter d'une nouvelle législation sur la cybersécurité en 2023, pilotée par l'Agence nationale de cybersécurité (CBS) qui notamment est chargée de sensibiliser les acteurs économiques aux menaces cyber, renforcer la réponse aux incidents, améliorer les capacités d'application de la loi et accroître la conscience publique face aux risques.

Quant au Cambodge, au Laos et à la Birmanie, ils présentent des capacités cyber limitées et font face à des défis pour améliorer leur position en matière de cybersécurité en raison de la disponibilité des ressources, de l'infrastructure technologique et des priorités nationales.

Si les signes d'un renforcement de l'arsenal législatif et réglementaire dans les pays d'Asie du Sud-Est sont bien présents, les différences de degré de préparation au niveau national (la Malaisie se classe à la 22ème position de l'Index national de cybersécurité lorsque la Birmanie se classe à la 152ème position) et l'absence de normes harmonisées au niveau régional demeurent encore des obstacles significatifs pour la résilience de la zone face à l'accélération des cybermenaces.

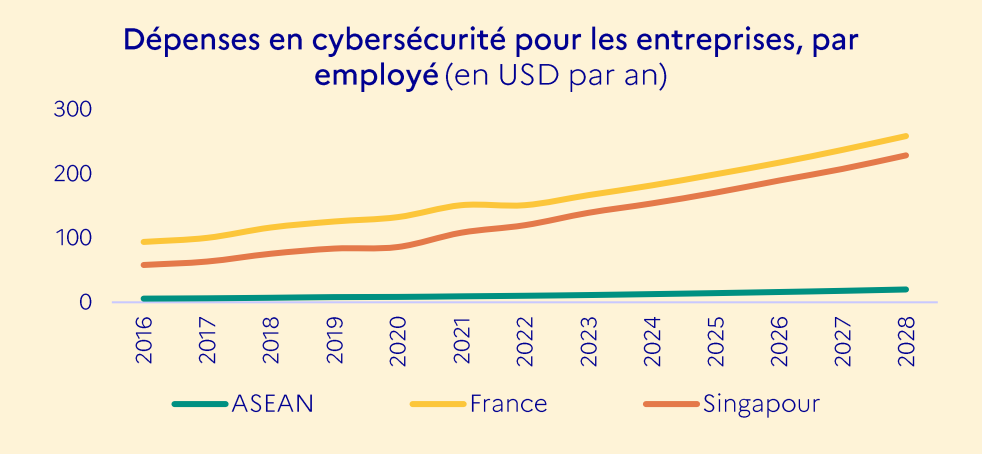


Graphique élaboré à partir des données de l'Index national de cybersécurité (NCSI) au 01/09/2023, du pilier « protection des données et cybersécurité » de l'Indice d'intégration numérique de l'ASEAN (ADII) au 01/08/2021 et de l'Indice Mondial de la Cybersécurité (GCI) en 2020. Pour chaque indice, le score maximum est de 100.

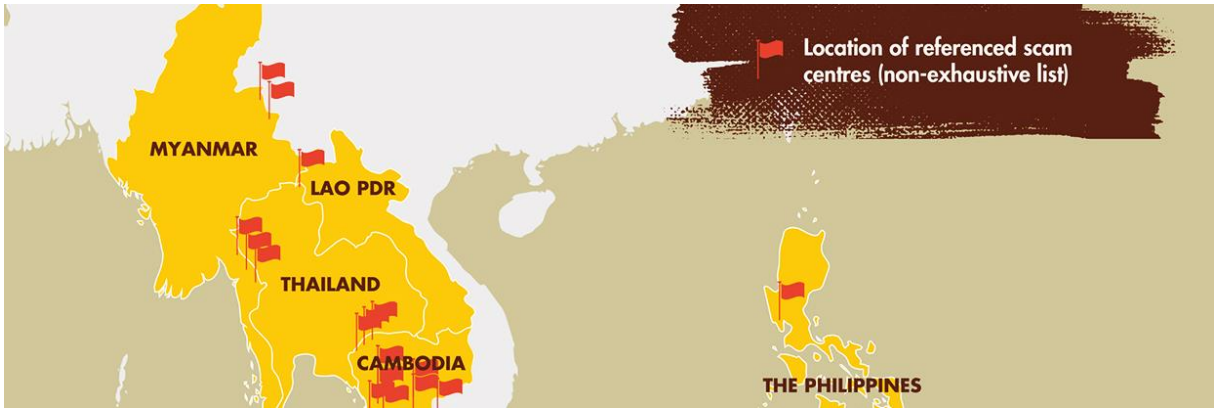
Pays hôte de l'INTERPOL Global Complex for Innovation (IGCI), un centre dédié à la lutte contre la cybercriminalité, Singapour est à l'initiative pour un renforcement de la collaboration régionale en matière de cybersécurité. Outre les initiatives nationales, l'ampleur et la nature transfrontalière des cybermenaces sont telles que la coopération régionale est devenue essentielle, les principales menaces affectant souvent plusieurs juridictions simultanément. Depuis 2016, Singapour est l'hôte de la Conférence ministérielle de l'ASEAN sur la cybersécurité (AMCC), une plateforme qui, bien qu'informelle, a été la première à faciliter le dialogue sur la cybersécurité au niveau ministériel dans la région. Dès l'année suivante, les pays de l'ASEAN ont adopté leur Stratégie de Coopération en Cybersécurité couvrant la période 2017-2020 ; une première feuille de route pour une collaboration régionale visant à sécuriser le cyberespace dans la région. Celle-ci a été révisée pour la période 2021-2025 et devrait être mise-à-jour mi-2024 pour s'adapter à l'évolution des cybermenaces, notamment avec l'utilisation accrue de l'IA générative, qui a pu abaisser la barrière d'entrée dans le paysage des menaces pour des acteurs moins sophistiqués. Plusieurs actions concrètes ont ainsi été initiées. Lancé en 2021, le Centre

d'Excellence en Cybersécurité et en Information (ACICE), dont le siège a été inauguré en juillet 2023 à Singapour, se veut « un centre de partage d'informations et de renforcement des capacités » qui permettra de « forger un consensus sur les 'règles de conduite' qui devraient régir le domaine numérique », selon le ministre de la Défense singapourien, Dr Ng Eng Hen. Annoncé dans la première Stratégie de Coopération de Cybersécurité (2017-2020), Singapour travaille également à la création d'un CERT (Computer Emergency Response Team) de l'ASEAN basé sur son territoire. Celui-ci devrait permettre une coordination plus forte de la réponse aux incidents de cybersécurité régionale et une coopération pour la protection des infrastructures d'information critiques (CII), y compris pour les CII transfrontalières, dont les secteurs bancaire/finance, les TIC et les transports (aviation et maritime). Malgré ces efforts de coopération, largement poussés par la cité-Etat, il n'existe pas encore de garantie d'aboutir à un cadre législatif unifié en Asie du Sud-Est[10]. La mise en œuvre des stratégies de cybersécurité reste fortement dépendante des initiatives individuelles des États membres, qui reflète la diversité de leurs économies et niveaux de maturité numérique. Les priorités ne convergent donc pas dans la résolution des problèmes de cybersécurité, tandis que le partage opportun de données sensibles est entravé par des préoccupations liées à la sécurité nationale. Cette diversité d'approches peut créer un manque d'interopérabilité entre les États membres, fragmentant l'architecture régionale de cybersécurité.

Entre le manque de ressources et la prévalence du crime organisé dans certains pays, des défis persistent dans la mise en œuvre d'une résilience contre les cybermenaces. Les engagements financiers des organisations, publiques et privées, dans l'Asie du Sud-Est en matière de sécurité numérique restent insuffisants. En 2023, les entreprises des pays de l'ASEAN allouaient en moyenne 11,32 USD par employé dans la cybersécurité, soit 15 fois moins que les 167,10 USD investis par leurs équivalents français. Les entreprises singapouriennes se démarquent cependant dans la région, se rapprochant des niveaux de dépense français avec un investissement moyen de 139,50 USD par employé en cybersécurité.



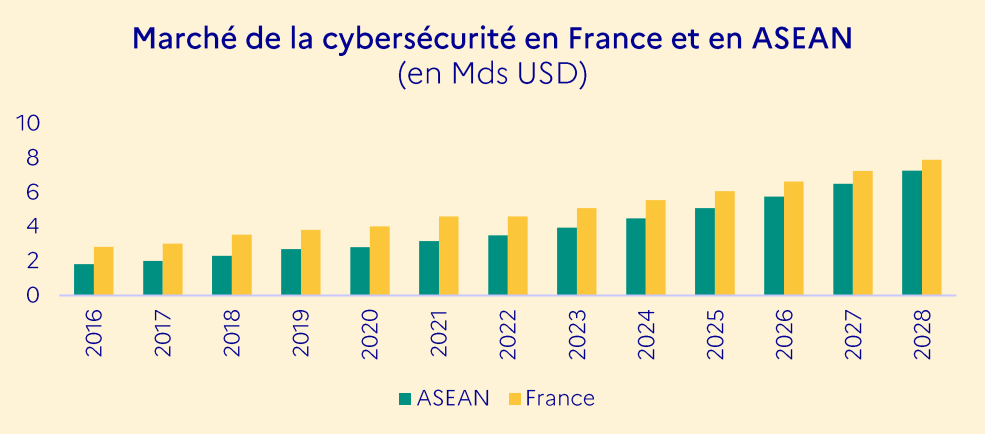
Le recrutement de personnels qualifiés représente lui-aussi un défi majeur pour de nombreux pays, notamment visible aux Philippines, classées parmi les 30 nations les plus ciblées par les cyberattaques à l'échelle mondiale et cible récurrente d'APT chinois[11]. Avec près de 120 millions d'habitants, le pays ne dispose que d'une équipe gouvernementale de réponse aux cyberattaques (CERT-PH) de 35 membres, poussant les autorités à collaborer avec des hackers « black hat », connus pour leurs attaques antérieures contre des sites gouvernementaux[12]. Enfin, la présence de réseaux cybercriminels en Asie du Sud-Est amplifie la cybermenace dans la région. En août dernier, un rapport[13] publié par le Haut-Commissariat aux droits de l'homme (HCDH) indiquait que des centaines de milliers de personnes étaient contraintes par des réseaux criminels à s'engager dans des activités illicites en ligne en Asie du Sud-Est, dont des escroqueries amoureuses, des fraudes aux cryptomonnaies et des jeux d'argent illégaux. Ces centres d'escroqueries, principalement localisés en Birmanie, au Cambodge, au Laos, aux Philippines et en Thaïlande, généreraient des milliards de dollars américains de revenus chaque année. Les victimes de ces trafics en ligne proviennent de l'ensemble de la région ASEAN, de la Chine continentale, Hong Kong, Taiwan, d'Asie du Sud, et même d'Afrique et d'Amérique latine.

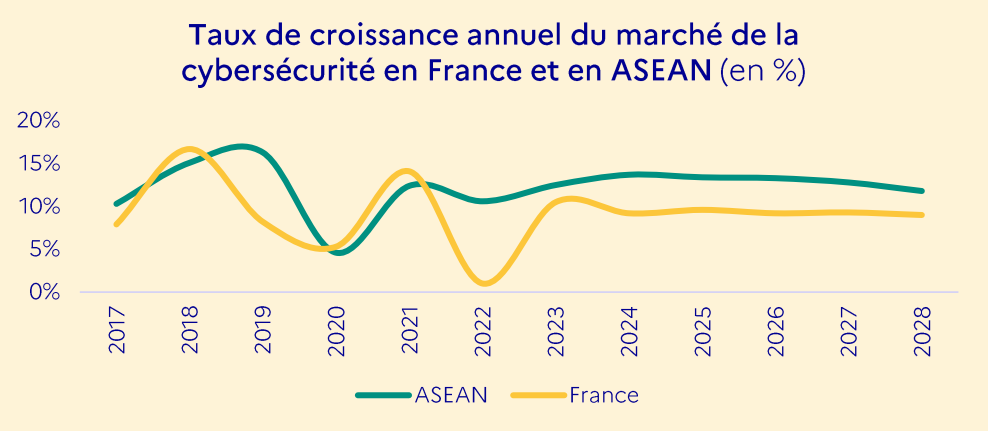


Des centaines de milliers de personnes sont victimes de trafic pour travailler dans des escroqueries en ligne en Asie du Sud-Est, selon un rapport des Nations unies. Crédit : HCDH.

Des opportunités économiques et de développement pour la France et ses entreprises dans la région

Le marché de la cybersécurité est en forte croissance dans l'Asie du Sud-Est, poussé par l'accélération de l'adoption de nouvelles solutions de cybersécurité. Le marché de la cybersécurité dans les pays de l'ASEAN devrait atteindre 4,49 Mds USD en 2024, avec une projection de 7,27 Mds USD d'ici 2028[14], soit un taux de croissance annuel composé (TCAC) de 12,80% sur la période 2024-2028.





Cette dynamique de croissance est principalement stimulée par l'expansion rapide du marché des solutions et produits de cybersécurité (pare-feu, antivirus, systèmes de détection d'intrusion, programmes de cryptage)[15], dont les revenus pourraient doubler dans les quatre prochaines années, passant de 2,14 Mds USD en 2024 à 4,07 Mds USD en 2028. Cette forte progression (17,43%) contraste avec celle plus modérée (8,02%) des services et conseils en sécurité informatique (audit et évaluation des vulnérabilités, gestion et réponse aux incidents de sécurité, formation des employés en cybersécurité)[16]. La maturité des marchés de la cybersécurité diffère toutefois au sein de l'ASEAN : Singapour bénéficie d'un marché développé et compétitif, desservant des clients locaux et globaux, tandis que des économies en développement telles que l'Indonésie

(5,0% de croissance du PIB en 2023), le Vietnam (5,0%) et la Thaïlande (1,9%) connaissent une numérisation accélérée, incitant à l'adoption initiale de solutions de cybersécurité avancées tant dans le secteur privé que public. En détail, pour 2024, le marché indonésien (280 millions d'habitants) devrait générer 2,41 Mds USD, soit la moitié du marché régional, suivi de Singapour avec 570 M USD, de la Malaisie avec 510 M USD, de la Thaïlande avec 380 M USD, et du Vietnam avec 310 M USD. En comparaison, le marché français, bien plus mature, devrait atteindre 5,56 Mds USD en 2024 et jusqu'à 7,92 Mds USD en 2028. La domination des entreprises américaines est incontestable dans le secteur en ASEAN, où elles captent plus de 90% des parts de marché[17]. Parmi les acteurs qui détiennent le plus de parts de marché dans la région (3,51 Mds USD), Microsoft occupe la première place (18%), suivi d'IBM (14%) et de Broadcom (9%). L'entreprise de services numériques (ESN) française, Capgemini, représente 2% de ce marché. L'ESN détient toutefois une part significative de 13% du marché singapourien de la cybersécurité (440 M en 2022), plaçant ainsi Capgemini au même niveau qu'IBM (14% des parts à Singapour). Les entreprises françaises telles qu'Orange Cyberdefense, ATOS (Eviden), Thalès ou IDEMIA disposent elles-aussi d'une présence dans la région, en particulier à Singapour où elles ont établi pour certaines leur siège pour la région Asie-Pacifique. Plusieurs startups françaises (ou fondées par des Français) sont également installées à Singapour, comme YesWeHack (French Tech 2030), TEHTRIS, Hackuity, XRATOR ou Secure-IC. La communauté French Tech à Singapour, regroupant 1 500 membres, compte également un chapitre dédié à la cybersécurité, favorisant ainsi la connexion des écosystèmes français et singapouriens sur cette thématique.

Singapour renforce sa position de leader en cybersécurité face aux défis de l'IA. La généralisation de l'utilisation de nouvelles technologies, comme l'IA générative, amplifie les risques de cybersécurité, tant sur la surface à protéger que sur l'intensité des attaques. Singapour, où l'économie numérique contribue à presque un cinquième du PIB, entend se positionner en chef de file pour contrer ces menaces émergentes. Créé en 2018 et basé à Singapour, le hub ICE71 (Innovation Cybersecurity Ecosystem Block71), premier centre dédié aux startups de la cybersécurité dans la région, illustre cet engagement. Né de la collaboration entre Singtel Innov8, le bras de capital-risque de Singtel, et NUS Enterprise, la branche entrepreneuriat de l'Université Nationale de Singapour (NUS), ICE71 aide au développement et à la croissance des startups spécialisées en cybersécurité. A l'échelle du pays, Singapour compte une quarantaine de startups spécialisées en cybersécurité[18], dont les deux tiers ont été créées au cours des cinq dernières années. Un quart de ces startups indique utiliser l'intelligence artificielle (IA) dans leur solution. Pour mémoire, Singapour dispose de l'écosystème de startup le plus dynamique de la zone, avec plus de 6 400 startups, soit la moitié de l'Asie du Sud-Est.

Crédit photo : Freepik.

Le cloud à Singapour

Technologie qui permet d'utiliser des serveurs à distance pour stocker, gérer et traiter des données, le « cloud computing » connaît une expansion spectaculaire à Singapour, dont la taille du marché (7,33 Mds USD ; 1,5% du PIB) a été multipliée par sept depuis 2016. Cette croissance est largement soutenue par les investissements du Gouvernement dans le secteur, qui a consacré un tiers de son budget informatique aux applications cloud en 2023, et par la collaboration avec les trois principaux fournisseurs de services cloud américains, Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP), qui se partagent 55% du marché du cloud à Singapour. Les acteurs chinois tels qu'Alibaba et Huawei peinent à s'imposer dans ce paysage oligopolistique dominé par les américains.

Ville la plus « smart » d'Asie[19], Singapour veut mettre le numérique au cœur de la vie de ses citoyens (« Digital to the Core ») et mise sur une adoption massive du cloud par ses agences gouvernementales, accompagné par les trois « hyperscalers » américains Amazon, Microsoft et Google. Dans son Plan directeur du numérique[20] (« Digital Government Blueprint ») de 2018, l'Agence gouvernementale de technologie de Singapour (« GovTech »), créée en 2016 sous la tutelle du Premier Ministre[21], s'est fixé l'objectif de migrer au moins 70% des systèmes gouvernementaux éligibles (non-sensibles) vers le cloud commercial d'ici 2023[22]. Avec un tiers du budget informatique pour 2023 (2,45 Mds USD) dédié au développement des applications cloud (743 M USD), Singapour a réalisé cet objectif[23]. Le succès de cette transition repose en grande partie sur le lancement de la plateforme Government on Commercial Cloud (GCC) en 2019, mise à jour en 2022 (GCC 2.0). S'appuyant sur les infrastructures des trois acteurs les plus importants du marché global, Amazon Web Services, Microsoft Azure et Google Cloud Platform, la plateforme « cloud-agnostic » (compatible avec plusieurs fournisseurs de services cloud qui permet aux agences de basculer facilement d'un fournisseur à un autre sans avoir à modifier fondamentalement l'architecture ou le fonctionnement de l'application) a permis d'accélérer la migration vers le cloud de plus de 600 services numériques gouvernementaux (MyCareersFuture, GoBusiness, SupplyAlly, Whole of Government Application Analytics, SHIP-HATS). La collaboration avec les acteurs privés fait ainsi partie intégrante de la stratégie du gouvernement. En 2023, les partenariats avec le secteur privé ont représenté près de la moitié (45%) des dépenses dans les applications cloud du gouvernement, en augmentation par rapport à 2022 (27%).

La migration des services numériques gouvernementaux vers le cloud permet d'optimiser les coûts et d'accélérer le développement des applications, ce qui se traduit par une plus grande satisfaction de la population à l'égard de ces services. D'après le directeur général de GovTech, Kok Ping Soon, la migration des charges de travail du gouvernement vers le cloud a généré des économies de coûts moyennes de 30 à 40% par rapport au maintien de ces systèmes sur site (« on premise ») et a multiplié la vitesse de développement des applications informatiques de 3 à 14 fois[24]. Cette transition vers le cloud ne représente pas simplement un changement en surface ; elle se manifeste par une utilisation plus répandue des services gouvernementaux numériques, accélérée également par la pandémie de Covid-19 (95% des interactions avec les services publics singapouriens ont été réalisées entièrement en ligne) et une satisfaction accrue des citoyens à cet égard (84% des citoyens et 79% des entreprises se disent soit « très satisfaits », soit « extrêmement satisfaits » des services gouvernementaux numériques à Singapour en 2022, contre respectivement 78% et 69% en 2018[25]).

Entre souveraineté numérique et démocratisation de l'intelligence artificielle (IA), les « hyperscalers » ont été des partenaires stratégiques du gouvernement pendant l'année 2023. En mai 2023, le Smart Nation and Digital Government Office (SNDGO) – qui regroupe Smart Nation et GovTech – et Google Cloud Platform ont annoncé le lancement de l'Artificial Intelligence Government Cloud Cluster (AGCC), une plateforme conçue pour i) accélérer l'adoption de l'IA dans le secteur public de Singapour ; ii) faire progresser les efforts de recherche en IA appliquée ; et iii) soutenir la croissance de l'écosystème local de startups qui utilisent cette technologie. Pionnière sur cette plateforme, l'équipe Open Government Products de GovTech, qui se définit elle-même comme une « équipe interne d'ingénieurs, de designers et de chefs de produits qui développent des technologies pour le bien public », y a développé son propre outil d'IA générative, Pair, qui offre aux fonctionnaires singapouriens une alternative sécurisée (et souveraine) aux grands modèles de langage (LLM) comme ChatGPT. Parallèlement, en août 2023, AWS a annoncé la création de Dedicated Local Zones, « conçues pour une utilisation exclusive par un client ou une communauté, et localisées dans un emplacement ou un centre de données spécifié par le client afin de se conformer aux exigences réglementaires »[26]. Le Smart Nation and Digital Government Group (SNDGG, renommé Smart Nation Group depuis octobre 2023) de Singapour sera le premier à déployer ce type d'infrastructure. À ce propos, le directeur de la technologie numérique du gouvernement de Singapour, Chan Cheow Hoe, a déclaré que « le SNDGG a collaboré avec AWS pour définir et créer des Dedicated Local Zones afin de nous aider à répondre à nos exigences strictes en matière d'isolation et de sécurité des données, permettant ainsi à Singapour d'exécuter des charges de travail plus sensibles dans le cloud en toute sécurité ». Ces zones dédiées viendront ainsi compléter le GCC qui gère les charges les moins critiques.

Le Gouvernement n'est pas le seul à miser sur le cloud. De plus en plus d'entreprises sont influencées par les politiques gouvernementales dans le domaine – 6 PME sur 10 à Singapour se disent « clairement influencées » par celles-ci[27] – et choisissent de migrer leurs charges de travail vers le cloud. Ainsi, en 2023, le marché du cloud public à Singapour a connu une croissance dynamique de 36% par rapport à l'année précédente, et représente près de la moitié du marché total de l'ASEAN (15,62 Mds USD en 2024)[28]. Le chiffre d'affaires du marché du cloud public devrait atteindre 7,33 Mds USD en 2024, soit 1,5 point de PIB, contre 990 M en 2016. L'IaaS (« Infrastructure-as-a-Service »), qui est l'infrastructure du cloud, domine le marché avec un volume prévu de 2,89 Mds USD en 2024, devant le PaaS (« Platform-as-a-Service »), une couche de virtualisation (« middleware ») ajoutée à l'IaaS, dont le volume d'affaires devrait atteindre 2,57 Mds USD la même année. Le marché du SaaS (« Software-as-a-Service »), qui est la

dernière strate du cloud, c'est-à-dire le logiciel ou l'application (comme Microsoft 365 ou Google Workspace) est estimé à 871 M en 2024. Entre 2024 et 2028, le volume d'affaires global du cloud public à Singapour devrait croître annuellement de 14,32% (contre 11,37% au niveau mondial), porté par l'essor du IaaS (16,75%) et du PaaS (17,09%), pour dépasser les 10 Mds USD de revenus dans trois ans, avec 11,19 Mds USD prévus en 2027. Tendance observée au niveau mondial, les trois « hyperscalers » américains dominent plus de la moitié du marché du cloud (IaaS, PaaS et SaaS) à Singapour : Amazon Web Services (AWS) capte 30% de ce marché, suivi de Microsoft Azure (15%) et de Google Cloud Platform (10%). Alibaba Cloud, premier acteur non-américain avec 5% de parts de marché, suscite un intérêt croissant pour le marché singapourien du cloud ; et notamment celui du secteur public (GCC). En 2022, l'entreprise chinoise assurait déjà être en collaboration avec plusieurs agences gouvernementales sur des projets impliquant notamment l'IA[29]. Toutefois, à l'échelle du pays, les acteurs américains restent encore largement privilégiés. Dans le seul marché du IaaS, les trois acteurs américains représentent à eux seuls 73% de la part totale (AWS : 45% ; Azure : 15% ; GCP : 13%), tandis qu'Alibaba Cloud et Huawei Cloud, cumulativement, ne représentent que 12%.

Crédit photo : Unsplash.

Les centres de données à Singapour

La puissance déployée par les centres de données installés à Singapour devrait dépasser un gigawatt (GW) en 2024, soit 60% des capacités totales en Asie du Sud-Est, pour un volume de marché estimé à 4 Mds (0,8% du PIB). Conséquence directe du moratoire entre 2019 et 2022 ayant suspendu la construction de nouveaux centres de données dans la cité-Etat, en raison de leur électro-intensivité (7% de la consommation d'électricité dans le pays), le rythme d'installation de nouveaux centres de données y a ralenti (seuls 332 MW sont prévus à la construction dans la cité-Etat) ce qui a profité à son voisin la Malaisie : à Johor Bahru, face à Singapour de l'autre côté de la frontière, où les capacités installées pourraient passer de 34 MW en opération à 491 MW, et dans la capitale à Kuala Lumpur (94 MW installés pour 594 MW prévus).

Dans les cinq prochaines années, les consommateurs et les entreprises généreront deux fois plus de données que toutes celles créées au cours des dix dernières années[30]. En conséquence, la capacité de stockage totale dans les centres de données et les appareils terminaux devrait elle aussi doubler entre 2023 et 2027 au niveau mondial. En fournissant l'infrastructure nécessaire pour stocker, traiter et distribuer les données qui alimentent les applications et services numériques modernes, les centres de données jouent un rôle central dans la transformation numérique.

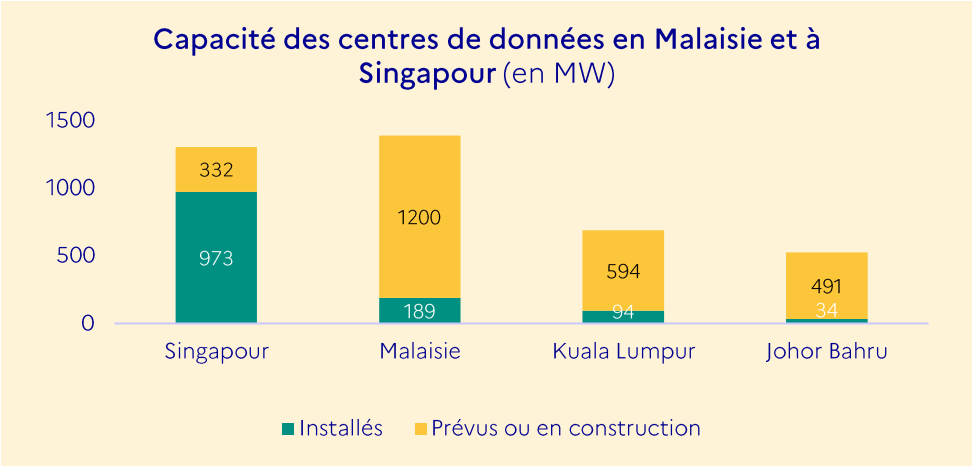
Malgré des prix de l'immobilier plus élevés et des coûts de construction et d'exploitation supérieurs à ceux pratiqués par ses voisins, Singapour s'est rapidement affirmé comme une destination privilégiée pour l'installation de centres de données, notamment grâce à son niveau de maturité technologique (en cinquième position de l'Indice mondial de l'innovation 2023[31]) et son attractivité auprès des investisseurs étrangers (climat des affaires, incitations fiscales, hub logistique et financier). Sa position géographique stratégique, située sur la principale façade maritime du monde, et ses infrastructures de télécommunications (nœud de 25 câbles sous-marins) ont contribué à attirer des géants mondiaux du numérique – américains, chinois et européens – renforçant son rôle clé dans le secteur.

Dans ce marché en croissance (4 Mds USD ; 0,8% du PIB), un opérateur français se distingue : OVHcloud. A Singapour, le marché des centres de données est estimé à plus de 4 Mds USD en 2024 et devrait atteindre 7,75 Mds USD en 2029. Celui-ci devrait croître de 13,9% par an entre 2024 et 2029, contre 18,1% entre 2017 et 2023[32]. Spécialisés dans la location d'espace et d'infrastructures pour héberger les serveurs et équipements informatiques de leurs clients, les opérateurs de colocation de centres de données tels que STT Global Data Centres (SG ; qui représente 12,4% des parts de marché en 2023), Equinix (US), Digital Realty (US), Singtel (SG), AirTrunk (AUS), Keppel DC (SG) et Global Switch (UK), cumulent ensemble plus de la moitié (55%) de la capacité opérationnelle (973 MW en 2023) à Singapour[33]. OVHcloud (FR) a inauguré en novembre 2023 son deuxième centre de données à Singapour d'une capacité de 2 MW (soit 0,2% de la puissance totale installée à Singapour), le premier de la région à déployer la technologie propriétaire d'OVHcloud de refroidissement des serveurs à l'eau (« watercooling »), permettant à ses centre de données de se passer d'air conditionné et donc de présenter des indicateurs de performance environnementale parmi les meilleurs de l'industrie (« Power Usage Efficiency »[34], PUE, de 1,29 contre 1,47 en moyenne à Singapour). Ce nouveau centre de données est l'un des premiers à être inauguré depuis la levée du moratoire sur la construction de nouveaux datacenters à Singapour.

Face à l'augmentation jugée trop importante de la demande énergétique des centres de données, les autorités singapouriennes ont mis sur pause leur développement entre 2019 et 2022. Principalement générée à partir de gaz naturel[35] (95%), l'électricité utilisée par les centres de données à Singapour représentait 7% de la consommation d'électricité dans le pays en 2020[36] (contre 1 à 2% en moyenne au niveau mondial), avec une projection à 12% d'ici 2030. L'Infocomm Media Development Authority (IMDA), en charge de réglementer le secteur des technologies de l'information et de la communication (TIC), a instauré un moratoire en 2019 suspendant la construction de nouveaux centres de données dans la cité-Etat ; il a été officiellement levé en janvier 2022. Durant cette période, l'IMDA et l'Economic Development Board[37] (EDB) ont travaillé conjointement à l'élaboration d'un Programme d'évaluation de l'empreinte carbone des centres de données (DC-CFA) qui vise à encourager le déploiement de centres de données à faibles émissions de carbone sur le territoire. De nouvelles conditions strictes sont dorénavant imposées pour la construction de nouveaux centres de données, notamment un plafond de 60 MW par an pour la construction et un PUE de 1,3 ou moins[38]. En 2023, les deux agences ont attribué des droits de développement pour de nouveaux projets de centres de données d'une capacité totale de 80 MW à quatre entreprises : deux américaines (Equinix et Microsoft), une chinoise (GDS Holdings) et une joint-venture entre le chinois ByteDance et l'australien AirTrunk[39]. Ces 80 MW ont contribué au pipeline de développement de plus de 300 MW.

Toutefois, ces capacités en développement ne parviennent pas à satisfaire la croissance de la demande de stockage de données à Singapour. Wong Wai Meng, PDG de Keppel Data Centres, l'un des acteurs les plus importants du marché, estime que la nouvelle limite de capacité (60 MW par an) est « insuffisante » pour répondre à la forte demande des entreprises[40]. Selon l'entreprise, la demande totale de capacité à Singapour dépassera les 3 GW d'ici 2030, soit trois fois la capacité actuellement installée (1 GW). Dès avril 2022, quatre mois après la levée du moratoire, l'association SGTech estimait que Singapour avait virtuellement perdu une capacité de 200 MW entre 2019 et 2021[41]. Entre 2010 et 2015, 12 installations totalisant 307 MW ont été construites, puis entre 2015 et 2020, 14 installations pour 768 MW, soit une moyenne annuelle de 150 MW, dépassant largement le nouveau quota de 60 MW. La forte augmentation de la demande de centres de données, accélérée par l'adoption du « cloud » et le développement de l'intelligence artificielle, dépassera ainsi l'offre future, affectée par le quota actuel.

Le moratoire singapourien a contribué à accélérer la montée en puissance de son voisin direct, la Malaisie, qui enregistre la plus importante croissance de la région dans le secteur. Avec 1,2 GW de développement en cours, la Malaisie, qui compte actuellement une capacité opérationnelle de 189 MW (soit 19% de la capacité actuellement déployée par les centres de données à Singapour), devrait multiplier par sept sa capacité au cours des cinq prochaines années, et ainsi dépasser Singapour[42].



Source : Cushman and Wakefield (2024). APAC Data Center Update: H1/H2 2023. Données du second semestre (S2) 2023 pour Singapour et Kuala Lumpur et du premier semestre (S1) 2023 pour Johor Bahru. Il est probable que des projets de centres de données aient été annoncés à Johor Bahru depuis cette période, les capacités pour Johor Bahru indiquées ci-dessus sont donc probablement sous-estimées. L'écart entre la capacité totale pour la Malaisie (189 MW ; 1 200 MW) et la somme des capacités de Kuala Lumpur et de Johor Bahru (128 MW ; 1085 MW) tient au fait que les villes malaisiennes moins importantes n'ont pas été incluses dans le tableau.

Nouveau point central pour les investisseurs dans les centres de données en Malaisie, l'état de Johor (voisin direct de Singapour) devrait attirer près de 5 Mds USD d'investissements supplémentaires dans les centres de données en 2024[43]. Face à Singapour, la Malaisie présente plusieurs caractéristiques qui en font une candidate idéale pour le développement d'un hub régional pour les centres de données : **i)** la disponibilité étendue et le coût abordable des terrains (coût d'acquisition du terrain estimé à 624 USD/m2 à Johor Bahru, 1 955 USD/m2 à Kuala Lumpur contre 11 573 USD/m2 à Singapour ; coûts de construction d'un centre de données estimé à 8,52 M USD/MW en Malaisie contre 11,23 M USD/MW à Singapour[44]) ; **ii)** une infrastructure électrique fiable, dense, affichant une surcapacité de l'offre avec des tarifs d'électricité abordables (0,10 USD/kWh contre 0,27 USD/kWh à Singapour[45]) ; **iii)** un accès facile à une main-d'œuvre qualifiée et plus abordable ; et **iv)** des politiques gouvernementales favorables aux entreprises (incitations fiscales dans le cadre du plan MyDIGITAL 2021-2030)[46]. D'autres facteurs tels que la disponibilité en eau et la considération des risques liés aux catastrophes naturelles, des éléments cruciaux dans la sélection des emplacements pour la construction de centres de données, renforcent l'attrait de la Malaisie pour les entreprises en quête de localisations idéales pour leurs installations.

Notes

La cybersécurité en Asie du Sud-Est

[1] Orange Cyberdefense (2023). Security Navigator 2024. Selon Orange, la « cyber-extorsion est une forme de cybercriminalité qui consiste à compromettre la sécurité d'un actif numérique d'une entreprise (confidentialité, intégrité ou disponibilité) et exploite la vulnérabilité ainsi créée pour extorquer un paiement ». Disponible ici.
[2] Statista (2023). Cybersecurity and cybercrime in the Asia-Pacific region. Disponible ici.
[3] IBM (2023). Cost of a Data Breach Report 2023. Disponible ici.
[4] Cyfirma (2023). Singapore and Southeast Asia: Threat Landscape. Disponible ici.
[5] Wired (2023). China Is Relentlessly Hacking Its Neighbors. Disponible ici.
[6] Forescout (2024). 2023 Global Threat Roundup Report. Disponible ici.
[7] Positive Technologies (2023). Cybersecurity threatscape of Asia: 2022–2023. Disponible ici.
[8] Lloyd's, Aon, MSIG, SCOR, TransRe et CyRiM (2019). Shen Attack: Cyber risk in Asia Pacific ports. Disponible ici. Dans le rapport, « l'attaque Shen » décrit trois scénarios dans lequel une attaque est lancée via un virus informatique transporté par des navires, qui brouille ensuite les registres de base de données des cargaisons dans les principaux ports, entraînant ainsi une perturbation sévère des activités.
[9] The Star (2022). Maritime Industry is the backbone of the Malaysian economy, says Transport Minister. Disponible ici.
[10] En 2021, les pays de l'ASEAN ont adopté le Cadre de Gestion des Données de l'ASEAN (DMF, un cadre similaire au RGPD européen) et les Clauses Contractuelles Types (MCC). Ils ont été développés pour coordonner les pratiques de gestion des données et les normes de transfert de données transfrontalières dans la région. Bien que ces documents soient consultatifs et ne requièrent pas de modifications législatives immédiates, ils encouragent malgré tout les entreprises à se conformer à un cadre commun.
[11] Surfshark (2023). Data breach statistics: Q3 2023. Disponible ici.
[12] Bloomberg (2024). Philippines Turns to Hackers for Help as US Warns of China Cyber Threat. Disponible ici.
[13] Haut-Commissariat des Nations unies aux droits de l'homme (2023). Online scams operations and trafficking in to forced criminality in Southeast Asia: recommendations for a human rights response. Disponible ici.
[14] Statista (2023). Market Insights on Cybersecurity – ASEAN. Disponible ici.
[15] Selon la méthodologie retenue par Statista, les solutions et produits de cybersécurité (« cyber solutions ») incluent la sécurité des applications (Microsoft, Broadcom, Check Point), la sécurité du cloud (Tenable, Trend Micro, Palo Alto), la sécurité des données (Commvault, Trellix, McAfee), la sécurité réseau (IBM, VMware, Netscout), la sécurité des terminaux (Crowdstrike, Qualys, Microsoft) et la gestion des identités (Okta, IBM, CyberArk). Exclut les services de sécurité professionnels, la sécurité physique, la continuité d'activité et les produits de sécurité gratuits.
[16] Selon la méthodologie retenue par Statista, les services et conseils en sécurité informatique (« security services ») incluent les services de sécurité gérés (Secureworks, Wipro, DXC Technology), l'externalisation de la cybersécurité (Deloitte, Infosys, TCS), le conseil en sécurité (Cognizant, IBM, Booz Allen Hamilton) et la planification et la formation en sécurité (CompTIA, SANS Institute, Infosec Institute). En revanche, elle exclut la sécurité physique (ADT, G4S, Allied Universal), la continuité d'activité et la reprise après sinistre (Quantum Corporation, HPE, IBM), les solutions spécifiques à la sécurité (Trend Micro, McAfee, Varonis) et le support ou la maintenance de logiciels propriétaires.
[17] Statista (2022). En prenant en compte uniquement la portion définie du marché, où 58% des parts sont clairement attribuées à des entreprises spécifiques, il apparaît que les acteurs américains dominent avec 97% de cette fraction. Cela signifie que, dans le segment identifiable du marché, une prépondérance des entreprises américaines est évidente. Toutefois, cette analyse ne tient pas compte des 42% restants, classés dans la catégorie « others », dont la répartition peut différer et influencer l'interprétation globale de la répartition du marché.
[18] StartupSG. Annuaire des startups, 2024. Disponible ici.

Le cloud à Singapour

[19] Institute for Management Development (2023). 2023 Smart City Index. Disponible ici.
[20] GovTech (2018 et mis à jour en 2020). Digital Government Blueprint. Disponible ici.
[21] GovTech est l'équivalent de la Direction interministérielle du Numérique (DINUM) en France. Service du Premier ministre, elle est placée sous l'autorité du ministre de la Transformation et de la Fonction publiques.
[22] A l'image de la doctrine du « Cloud au centre » du Gouvernement français, où le cloud devient dorénavant le mode d'hébergement et de production par défaut des services numériques de l'État.
[23] ZDNet (2023). Singapore focuses ICT spend on cloud applications. Disponible ici.
[24] GovInsider (2023). Singapore's digital government to prioritise industry collaborations, sustainable procurement, says Kok Ping Soon, Chief Executive of GovTech. Disponible ici.
[25] GovTech (2022). Annual Survey on Satisfaction with Government Digital Services (Citizens) - For 2022. Disponible ici.
[26] Amazon Web Services (2023). AWS Digital Sovereignty Pledge: Announcing new dedicated infrastructure options. Disponible ici.
[27] Vodien (2022). Singapore Business Report: The Rise of SME Cloud Adoption. Disponible ici.
[28] Statista (2023). Public Cloud – Singapore. Disponible ici.
[29] ZDNet (2022). Alibaba Cloud eyes Web3 potential, participation on Singapore government cloud. Disponible ici.

Les centres de données à Singapour

[30] JLL (2024). Data Centers 2024 Global Outlook. Disponible ici.
[31] Organisation mondiale de la propriété intellectuelle (2024). Indice mondial de l'innovation 2023. Disponible ici.
[32] Mordor Intelligence (2023). Singapore Data Center Market. Disponible ici.
[33] Cushman and Wakefield (2024). APAC Data Center Update: H2 2023. Disponible ici.
Les centres de données sont des installations qui nécessitent une quantité importante d'électricité pour alimenter les serveurs, les systèmes de refroidissement, l'éclairage et d'autres équipements essentiels au bon fonctionnement des infrastructures informatiques. On utilise souvent les mégawatts (MW) ou gigawatts (GW) comme unité de mesure pour évaluer la taille et la capacité des installations.
[34] Le PUE, ou « Power Usage Effectiveness », est un indicateur développé par le Green Grid pour évaluer l'efficacité énergétique d'un centre de données. Il se calcule en divisant la consommation totale d'énergie du centre de données par la consommation totale d'énergie des équipements informatiques (serveurs, stockage, réseau). En moyenne, si les centres de données singapouriens affichent un PUE de 1,5, ce qui signifie qu'il faut 1,5 watts à l'entrée du centre de données pour chaque watt consommé par les équipements informatiques.
[35] Energy Market Authority. What fuel is used to generate electricity in Singapore. Disponible ici.
[36] Ministry of Trade and Industry (2020).
[3737] Agence en charge de la promotion de l'attractivité de Singapour
[38] The Straits Times (2022). Singapore pilots sustainable way to grow data centre capacity. Disponible ici.
[39] The Business Times (2023). Government awards 80 MW of new capacity to 4 data centre operators in pilot exercise. Disponible ici.
[40] NIKKEI Asia (2023). Singapore risks losing new data center demand, Keppel warns. Disponible ici.
[41] The Straits Times (2022). Conditions for data centre applications in S'pore insufficient, industry proposes own renewable energy grid. Disponible ici.
[42] Cushman and Wakefield (2024). APAC Data Center Update: H2 2023. Disponible ici.
[43] Yahoo! Finance (2023). Johor benefitting from a data centre boom. Disponible ici.
[44] Cushman and Wakefield (2023). Data Center Construction Cost Guide 2023/2024. Disponible ici.
[45] RHB Research (2023). Rise of Data Centres in ASEAN. Disponible ici.
[46] Service économique de Kuala Lumpur (2023).