LES PUBLICATIONS

[EN CLAIR]

LA PLACE DE LA FRANCE SUR LE MARCHÉ INDONÉSIEN DE LA CYBERSÉCURITÉ

Par Pierre-François BLIN & Nathan SALLAUD

LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

En pleine ascension, l'Indonésie se positionne comme un acteur significatif de la cybersécurité mondiale, attirant des partenariats globaux. Face à cette dynamique, de quelle manière la France, avec ses *leaders* technologiques, peut-elle s'impliquer dans la région asiatique et influencer sa stratégie de cybersécurité ? Cet article présente les défis de cybersécurité auxquels est confrontée l'Indonésie et les opportunités qui en découlent pour les sociétés françaises du secteur de la cybersécurité.

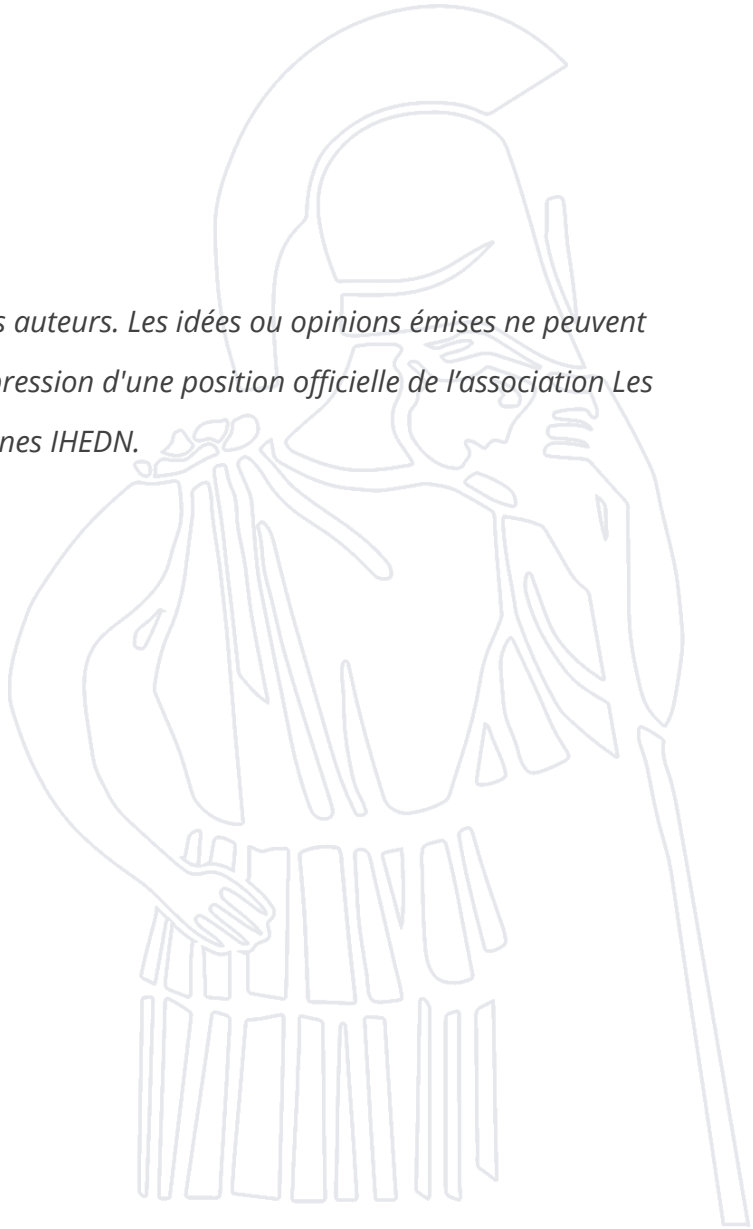
Cet « En Clair » s'inscrit dans le dossier relatif aux exportations d'armement de la France en Indopacifique. Coordonné et piloté par le pôle international des Jeunes IHEDN, ce dernier vise à alimenter les réflexions de l'ensemble des délégations internationales de l'association tout en y associant ses autres entités (comités d'étude et délégations régionales).

À PROPOS DES AUTEURS

Nathan SALLAUD est étudiant de l'ESSEC en stratégie et diplômé des Mines Saint-Étienne. Durant ses études et son engagement en tant que réserviste de l'armée de Terre, il développe un intérêt particulier pour la défense, la géopolitique et les relations internationales. Il est chargé de mission du pôle international des Jeunes IHEDN depuis 2023.

Pierre-François BLIN est consultant et doctorant en cybersécurité géomatique à l'Universitas Gadjah Mada (Yogyakarta-Indonésie). Il est délégué international des Jeunes IHEDN en Indonésie et membre du comité Cyber de l'association depuis 2021.

Ce texte n'engage que la responsabilité des auteurs. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.



La montée en puissance du marché de la cybersécurité en Indonésie

Malwares, infostealers, ransomwares, espionnage : les attaques cyber se multiplient dans le monde, avec une hausse de 38% de 2021 à 2022[1]. La région Asie-Pacifique n'est pas épargnée. En effet, celle-ci est, selon IBM, pour la seconde année consécutive, la région la plus impactée par les attaques cyber. Elle représente 31% du volume mondial des attaques recensées[2]. Pour l'Indonésie, la question de la cybersécurité ne peut donc pas être évitée, d'autant plus que la montée en puissance des *startups* indonésiennes ne fait que resserrer ses liens avec le monde digital et ses vulnérabilités[3].

En conséquence, le marché indonésien de la cybersécurité, actuellement sixième de la région[4] Asie-Pacifique, semble avoir de beaux jours devant lui avec des prévisions impressionnantes : une évolution anticipée de 2,05 en 2023 à 3,39 milliards de dollars américains d'ici 2028 selon l'*International Trade Administration*[5].

Pour contrer et anticiper l'impact des cyberattaques, le gouvernement indonésien met en œuvre des mesures ciblées. Ces mesures sont visibles sous trois formes principales.

- La première se traduit par des investissements gouvernementaux avec la création, notamment, d'agences spécialisées. Par exemple, la BSSN (l'agence crypto et cyber d'Indonésie) est recréée en 2017 ;

[1] « Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks ». Check Point [en ligne], 5 janvier 2023 [consulté le 14/11/23]. Disponible sur : https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/#:~:text=Global%20cyberattacks%20increased%20by%2038,-learning%20post%20COVID-19.

[2] « IBM Report: Asia-Pacific Felt the Brunt of 2022 Cyberattack ». *IBM India Newsroo* [en ligne], 22 février 2023 [consulté le 14/11/23. Disponible sur : https://in.newsroom.ibm.com/2023-02-22-IBM-Report-Asia-Pacific-Felt-the-Brunt-of-2022-Cyberattacks.

[3] « À travers l'économie d'un archipel : Dossiers thématiques des CCEF en Indonésie ». *Les conseillers du commerce extérieur de la France*, juillet 2023, n° 3, 24p.

[4] NURHAYATI-WOLFF, Hanadian. « Cybersecurity and cybercrime in Indonesia – statistics & facts ». *Statista* [en ligne], 12 décembre 2023 [consulté le 18/11/23.]. Disponible sur : https://www.statista.com/topics/11732/cybersecurity-and-cybercrime-in-indonesia/#topicOverview.

[5] « Market Intelligence: Indonesia cybersecurity ». *International Trade Administration* [en ligne], 7 mars 2023 [consulté le 18/11/23]. Disponible sur : https://www.trade.gov/market-intelligence/indonesia-cybersecurity.

- La seconde prend la forme de la mise en place d'infrastructures adaptées. Un exemple actuel renvoie à la modernisation de l'environnement cybernétique indonésien en vue des élections générales qui auront lieu en 2024[6] ;
- La troisième action se traduit enfin par la mise en place d'un cadre réglementaire approprié avec, par exemple, le projet de loi du deuxième amendement (RUU) à la loi n°11 de 2008. Cette loi concerne l'information et les transactions électroniques (ITE) par l'administration indonésienne[7].

Le marché indonésien de la cybersécurité : un marché à saisir pour les entreprises étrangères

Le besoin de cybersécurité est donc bien réel mais qu'en est-il des solutions locales ? Parmi les entreprises de cybersécurité indonésiennes, seules quelques entreprises nationales proposent des offres axées sur la sécurité des réseaux et sur la protection des données. *Xynexis Indonesia*, entreprise indonésienne spécialisée dans la cybersécurité, réalisant un peu plus de 6 millions de dollars de chiffre d'affaires[8], en est un exemple. Toutefois, ces solutions restent inadaptées face à des menaces très sophistiquées comme les attaques par *ransomware* (lesquelles représentent près de 9% des attaques recensées[9] dans la région Asie-Pacifique).

En effet, malgré leur dimension nationale, les entreprises indonésiennes sont limitées en termes de ressources (financières et humaines), impactant ainsi leurs performances, leur capacité d'innovation et leur réputation dans le pays. Le besoin indonésien de cybersécurité n'est donc pas entièrement satisfait face aux attaques complexes. Cela constitue une opportunité commerciale significative pour les acteurs étrangers de la cybersécurité, disposant de moyens généralement supérieurs.

[6] NURMALASARI, Novi. « BSSN's cybersecurity efforts for fair and safe 2024 general election ». *Indonesia business post* [en ligne], 31 mars 2023 [consulté le 20/11/23]. Disponible sur : https://indonesiabusinesspost.com/insider/bssns-cybersecurity-efforts-for-fair-and-safe-2024-general-election/.

[7] SANTHIKA, Eka. « Indonesia to Update Cybercrime Laws with Second Amendment to ITE Law ». *OpenGovAsia* [en ligne], 17 avril 2023 [consulté le 20/11/23]. Disponible sur : https://opengovasia.azurewebsites.net/indonesia-to-update-cybercrime-laws-with-second-amendment-to-ite-law/.

[8] « Xynexis Revenue and Competitors ». *Growjo* [en ligne], 2023 [consulté le 22/11/23]. Disponible sur : https://growjo.com/company/Xynexis.

[9] NURHAYATI-WOLFF, Hanadian. « Cybersecurity and cybercrime in Indonesia – statistics & facts », *op. cit*.

Ce besoin d'aide internationale a été illustré récemment. En mai 2023, le groupe *Lock Bit 3.0* a perpétré une attaque par rançongiciel contre la banque indonésienne *Syariah Indonesia* (BSI)[10]. Cela s'est traduit par la compromission de 1,5 térabytes de données personnelles appartenant à 15 millions de clients, ainsi que par la destruction d'infrastructures. Cette attaque, fragilisant grandement la BSI, a ouvert la porte aux Américains, plus réactifs et dotés de moyens plus importants pour résoudre le problème. De manière générale, ces entreprises étrangères, disposant de moyens plus conséquents et d'une expertise accrue, ont investi le marché indonésien ou y renforcent actuellement leur présence. Dans ce cadre, elles ne se contentent pas de soumettre des offres de solutions pertinentes. Elles s'engagent également dans des partenariats et des collaborations avec les acteurs locaux. Cela les conduit à combler les lacunes du pays, tout en renforçant leur intégration et leur impact sur le marché indonésien.

Par ailleurs, l'intégration d'acteurs étrangers dans le secteur de la cybersécurité en Indonésie est facilitée par la stratégie mise en place par le pays et la BSSN. Celle-ci a pour objectif d'augmenter le nombre de contrats avec des partenaires étrangers, permettant ainsi à l'Indonésie de diminuer sa dépendance vis-à-vis d'un cercle limité d'acteurs. Parmi cette diversité d'acteurs, figurent notamment *Cisco* (entreprise occidentale), *Kaspersky* (entreprise russe) et *Samsung* (entreprise asiatique). Comme expliqué précédemment, la stratégie du pays a permis une intégration effective de ces sociétés dans le paysage gouvernemental indonésien. Un exemple notable en est la société russe *Kaspersky* qui, en 2021, a conclu un accord de coopération, *Memorandum of Understanding,* avec la BSSN ; ce dernier visant à renforcer le développement de la cybersécurité dans le pays[11].

[10] AUDINA, Nur. « BSI's data breach: A menace to Indonesia's banking security ». *Indonesia business post* [en ligne], 16 mai 2023 [consulté le 22/11/23]. Disponible sur : https://indonesiabusinesspost.com/insider/bsis-data-breach-a-menace-to-indonesias-banking-security/.

[11] « Kaspersky and BSSN sign MoU to develop Indonesia's cybersecurity capability amidst rapid digitalization ». *Kaspersky* [en ligne], 21 juin 2021 [consulté le 24/11/23]. Disponible sur : https://www.kaspersky.com/about/press-releases/2021_kaspersky-and-bssn-sign-mou-to-develop-indonesias-cybersecurity-capability-amidst-rapid-digitalization.

La France, un acteur présent et reconnu dans un environnement concurrentiel

Les entreprises françaises sont naturellement présentes sur ce marché indonésien qui présente de multiples opportunités. À titre d'exemple, *Thales*, qui, grâce à sa présence sur le territoire depuis plus de quarante ans, a su développer son offre de cybersécurité en parallèle de ses activités principales[12]. *Thales* est, par ailleurs, bien implanté dans le pays, comme le démontre son investissement dans de nombreux projets indonésiens. Il est notamment fournisseur du *Indonesian Immigration Office* en matière de systèmes d'identification biométrique automatisés et fournisseur clé dans les solutions de villes intelligentes. Ces entreprises françaises, présentes sur le territoire indonésien, sont indéniablement reconnues à l'international pour leur expertise.

Néanmoins, d'autres facteurs sont à prendre en considération dans leur positionnement sur le marché (relations diplomatiques entre états, besoins locaux, etc.). Ces différents facteurs favorisent la concurrence entre les spécialistes internationaux de la cybersécurité. L'intervention américaine, à la suite de l'attaque de *Lock Bit 3.0* contre la banque BSI en 2023, le démontre parfaitement. En étant les premiers à intervenir, les Américains ont pu non seulement gagner en influence mais également négocier d'autres accords pour favoriser leurs solutions au détriment de leurs concurrents.

Néanmoins, cette concurrence n'est pas un frein aux partenariats entre rivaux. La collaboration entre *Orange Cyberdefense* et *Cisco* sur leur solution commune de protection de données *Umbrella*[13] le démontre parfaitement.

[12] « Thales in Indonesia ». ***Thales*** [en ligne], 2023 [consulté le 24/11/23]. Disponible sur : https://www.thalesgroup.com/en/countries/asia-pacific/thales-indonesia.

[13] « SASE solutions: Cisco technology meets Orange integration ». ***Orange Business*** [en ligne], 2023 [consulté le 24/11/23]. Disponible sur : https://www.orange-business.com/en/partners/sase-solutions-cisco-technology-meets-orange-integration.

Quelle stratégie française pour conquérir le marché cyber indonésien ?

Il est fondamental de reconnaître que l'Indonésie ne se résume pas à un simple marché additionnel pour la vente de solutions de cybersécurité et d'avions *Rafale*. En effet, avec ses plus de 280 millions d'habitants, l'Indonésie représente un partenaire de poids, bénéficiant d'une position géographique stratégique et constituant une voie d'accès importante au marché indopacifique. De plus, le pays dispose d'experts, essentiels au développement de solutions innovantes.

Par ailleurs, l'Indonésie adopte une approche de la résolution des problèmes cyber propice à la collaboration avec des acteurs étrangers. Le pays a souvent tendance à réagir aux événements au fil de leur survenance, plutôt que d'investir dans l'anticipation et la gestion des risques.

Ces différents facteurs offrent à l'Indonésie un potentiel incroyable et beaucoup l'ont compris. L'exemple de la société française *Tehtris*[14] l'illustre parfaitement. Cette société, cofondée par des anciens membres des services de renseignement français, réfléchit à l'Indonésie comme porte d'entrée du marché indopacifique avec l'aide, notamment, de la *French Tech Indonesia*[15]. Moins onéreuse que Singapour et tout aussi efficace pour pénétrer son marché, l'Indonésie cumule les avantages dans la région Asie-Pacifique. Néanmoins, la manière dont les entités françaises opèrent dans ce pays est perfectible. Comparée aux pays concurrents, la France ne se coordonne pas de la même manière. Elle pourrait ainsi exploiter à son avantage tout le potentiel de ses entités, qu'elles soient gouvernementales, académiques ou encore privées, par davantage de coopération.

[14] « COMEX ». *Tehtris* [en ligne], 2023 [consulté le 03/12/23]. Disponible sur : https://tehtris.com/fr/entreprise/comex/.

[15] « La French Tech Indonesia ». *La French Tech Indonesia* [en ligne], 2023 [consulté le 05/12/23]. Disponible sur : https://frenchtech.id/welcome.






publication@jeunes-ihedn.org