Le rôle de la cybersécurité et de la sécurité des données dans l'économie numérique

BRIEF

À mesure que les économies évoluent vers des modèles numériques et en ligne, les menaces peuvent rapidement dépasser les approches traditionnelles de la sécurité des données. Plus que jamais, les gouvernements et les organisations doivent être proactifs en créant et en adaptant des systèmes pour faire face à ces menaces. En protégeant leurs propres opérations, les informations des personnes qui utilisent leurs services seront également mieux protégées.

Cette note, rédigé en étroite collaboration avec Macmillan Keck, cherche à identifier les attributs spécifiques des cadres de cybersécurité et de sécurité des données qui peuvent aider les décideurs politiques et les régulateurs à construire une économie numérique qui inclut - et sert - tout le monde.

Février 2022

Macmillan Keck

Seharish Gillani,
Ahmed Dermish, and
Jeremiah Grossman
of the UNCDF
Policy Accelerator

Résumé

En 2020, le coût économique des violations de la sécurité des informations et des actifs technologiques s'élevait à un montant stupéfiant de 4 à 6 billions de dollars, soit environ 4 à 6 % du PIB mondial. La sécurité des données et la cybersécurité visent chacune à préserver la confidentialité, l'intégrité et la disponibilité des actifs informationnels. La plupart des cyberattaques sont motivées par des raisons financières. En général, un acteur de la menace s'infiltre dans le système cible, puis utilise un logiciel malveillant pour extraire des informations, retirer des fonds, demander une rançon ou commettre d'autres méfaits.

Le renforcement de la cybersécurité nécessite une action coordonnée. L'UIT a mis en place un programme de renforcement des capacités de cybersécurité pour les pays en développement.[1] Au moins 114 gouvernements nationaux ont adopté des stratégies de cybersécurité et 118 ont créé des équipes nationales de réponse aux incidents de sécurité informatique (CSIRT). Beaucoup ont créé des agences de cybersécurité et certains ont mis en place des CSIRT sectorielles pour protéger les infrastructures critiques. De nombreux pays mettent à jour leur législation pénale et renforcent l'application de la loi. La Convention sur la cybercriminalité du Conseil de l'Europe, qui favorise l'harmonisation internationale des enquêtes et de l'application des lois de cybercriminalité, a été ratifiée par 45 États membres et 22 États d'Afrique, des Amériques et d'Asie-Pacifique.

En outre, les organismes de normalisation nationaux et internationaux ont élaboré des cadres de gestion des cyberrisques. Les entreprises sont également de plus en plus nombreuses à créer leurs propres CSIRT internes. Les institutions publiques et privées ont mis l'accent sur la sensibilisation et l'éducation. Les pays développés investissent pour combler le déficit mondial de compétences en cybersécurité des travailleurs nécessaires.

Considérations à la lecture de cette note:

1. Quels sont les défis liés à la cybersécurité et à l'économie numérique les plus importants sur votre marché, à la fois a) en général et b) pour les groupes mal desservis tels que les femmes et les personnes à faibles revenus ?

2. Les réglementations de la cybersécurité et de la sécurité des données dans votre pays traitent-elles de :
   - **La numérisation :** L'application de la réglementation en matière de cybersécurité et de sécurité des données à l'économie numérique ?
   - **L'inclusivité :** Les défis spécifiques en matière de cybersécurité et de sécurité des données auxquels sont confrontés les femmes, les personnes à faibles revenus et/ou d'autres groupes mal desservis ?

3. Quelles sont les entités responsables de la réglementation de la cybersécurité et de la sécurité des données ? Les responsabilités sont-elles claires, et des mécanismes sont-ils en place pour éviter l'arbitrage réglementaire ? Dans la négative, comment cela pourrait-il être amélioré ?

Nature et importance de la sécurité des données et de la cybersécurité

Assurer la confidentialité, l'intégrité et la disponibilité des actifs informationnels

Les termes ***sécurité des données***[2] et ***cybersécurité***[3] sont souvent utilisés de manière interchangeable car ils visent tous deux à protéger les ***actifs informationnels*** (données et informations précieuses)[4] et à sécuriser les ***actifs technologiques*** (matériel, logiciels, systèmes, serveurs, réseaux et autres conteneurs électroniques qui collectent, traitent, transportent, stockent et récupèrent les actifs informationnels).[5] La distinction est subtile, la sécurité des données mettant l'accent sur la protection directe des actifs informationnels eux-mêmes et la cybersécurité sur la sécurisation des actifs technologiques en tant que moyen de protéger les actifs informationnels.

La sécurité des données et la cybersécurité visent à préserver la confidentialité, l'intégrité et la disponibilité des actifs informationnels d'une organisation. Dans ce contexte, la ***confidentialité*** signifie que l'accès aux actifs informationnels est limité aux personnes et aux systèmes autorisés ; ***l'intégrité*** signifie que les actifs informationnels restent dans l'état prévu par le propriétaire ; et la ***disponibilité*** signifie que l'accès aux actifs informationnels par les personnes et les systèmes autorisés est fiable.[6] Ces trois piliers de la sécurité sont connus sous le nom de ***triade CIA***.[7]

Un ***incident de sécurité*** est un événement qui compromet l'intégrité, la confidentialité ou la disponibilité des actifs informationnels, une ***violation de données*** est un incident de sécurité qui entraîne la divulgation de données confidentielles à une personne non autorisée, et une ***cyberattaque*** est une tentative non autorisée d'un ***acteur de la menace***[8] de compromettre des actifs informationnels ou technologiques.[9] Les menaces à la sécurité des actifs informationnels et technologiques sont aujourd'hui vastes et évolutives.[10]

L'importance croissante des actifs informationnels et technologiques

Les entreprises publiques et privées accumulent des volumes massifs et croissants d'actifs informationnels, tandis que les particuliers sont également de plus en plus nombreux à créer, collecter, partager et consommer des données.[11] Les entreprises et les particuliers s'appuient de plus en plus sur les actifs informationnels et technologiques pour fournir ou acquérir des biens, des services et des informations.[12] Les entreprises[13] et les particuliers[14] confient également leurs informations à d'autres entreprises ou particuliers à un rythme croissant. Dans les pays à revenu élevé comme dans les pays en développement, les particuliers adoptent les technologies numériques.[15] Le pourcentage de ménages des pays en développement disposant d'un ordinateur à domicile est passé de 15,6 % en 2005 à 36,1 % en 2019,[16] tandis que les abonnements de téléphonie mobile pour 100 personnes ont été multipliés par trois dans le monde et par quatre dans les pays à revenu faible ou intermédiaire entre 2005 et 2020.[17] En outre, en 2020, le nombre de comptes d'argent mobile enregistrés a augmenté de 12,7 % dans le monde pour atteindre 1,21 milliard de comptes, soit le double du taux de croissance prévu.[18]

La menace croissante des failles de sécurité

Les entreprises des pays en développement étant de plus en plus dépendantes des actifs informatiques et technologiques, elles sont

confrontées à des menaces de sécurité similaires à celles de leurs homologues des pays développés. Par exemple, il y a eu de nombreux incidents de sécurité liés aux services financiers numériques, tels que l'accès non autorisé de tiers aux systèmes d'information des entreprises, obtenu en incitant des employés peu méfiants à divulguer leurs informations de connexion au Ghana, au Kenya, en Tanzanie, en Ouganda et en Zambie, une panne pendant une mise à niveau du système au Zimbabwe et une attaque malveillante par déni de service au Kenya.[19] Plus largement, une entreprise de cybersécurité a signalé 24 millions d'incidents liés à des logiciels malveillants en Afrique en 2016,20 et la même année, le secteur financier du Ghana aurait connu à lui seul plus de 400 000 incidents liés à des logiciels malveillants.[21] Les infrastructures traditionnelles des pays en développement dépendent aussi de plus en plus des actifs informatiques et technologiques, notamment pour la surveillance et la gestion des réseaux électriques.[22] Les cyberattaques contre ces actifs sont en augmentation,[23] elles ont par exemple perturbé l'approvisionnement en électricité en Ukraine en 2015 et 2016[24] et en Afrique du Sud en 2019.[25]

Le coût économique des failles de sécurité

Les pertes monétaires directes mondiales dues à la cybercriminalité en 2020 ont été estimées avoir presque doublé, passant de 522,5 milliards de dollars en 2018 à 945 milliards de dollars,[26] tandis que les dépenses en cybersécurité en 2020 devraient dépasser 145 milliards de dollars,[27] représentant ensemble environ 1,3 % du PIB mondial.[28] En 2017, la cybercriminalité a coûté à l'Afrique des pertes directes estimées à 3,5 milliards de dollars.[29]

Ces estimations excluent les coûts indirects pour les victimes, tels que le coût d'opportunité, les temps d'arrêt, la perte d'efficacité, le dénigrement de la marque, la perte de confiance, la violation de la propriété intellectuelle et l'atteinte au moral des employés. Elles excluent également les coûts systémiques tels que les impacts sur la chaîne d'approvisionnement des fournisseurs en amont et des clients en aval. Le coût économique total de la cybercriminalité, y compris les coûts directs, indirects et systémiques en amont, a été estimé à trois fois son coût direct[30] - ce qui place le coût mondial total pour 2020 à près de 4 000 milliards USD, soit environ 4 % du PIB mondial. Ce chiffre est conforme aux estimations selon lesquelles le coût annuel global de la cybercriminalité s'élèvera à 6 000 milliards USD en 2021.[31]

Les entreprises des pays en développement sont confrontées à des pertes liées à la cybercriminalité hors normes, comme le braquage de 81 millions USD de la Bangladesh Bank en 2016. Ce vol a fait suite à des incidents antérieurs similaires en Équateur, en Inde, en Pologne, en Russie, à Taïwan et au Viêt Nam.32

Menaces et motivations

Motifs des acteurs de la menace

Il a été estimé que 70 % des incidents de sécurité en 2020 étaient motivés par des raisons financières et que le crime organisé était à l'origine de 80 % des violations de données.[33] Cependant, certains acteurs de la menace, appelés ***hacktivistes***, sont motivés par une idéologie politique, socioculturelle ou religieuse. En juin 2011, des hacktivistes ont attaqué le site web de MasterCard, provoquant sa panne, pour protester contre le blocage des paiements à WikiLeaks.[34] D'autres sont motivés par la vanité, la

vengeance, l'indignation ou d'autres objectifs non financiers.[35] Les acteurs de la menace parrainés par des États peuvent poursuivre des buts géopolitiques ou militaires par le biais du cyberespionnage, en interférant avec des élections étrangères ou en sabotant des services publics pour saper la stabilité politique des adversaires.[36]

Méthodes des acteurs de la menace

Les acteurs de la menace combinent souvent une série d'actions pour poursuivre leurs objectifs. La première étape consiste généralement à infiltrer le système cible en obtenant un accès non autorisé aux informations ou aux ressources technologiques. Parfois, l'accès est obtenu en utilisant des technologies pour pénétrer les ***pare-feu*** conçus pour empêcher les accès non autorisés. Un exemple est la violation de données de mars 2017 d'Equifax, l'agence mondiale d'évaluation du crédit, qui a exposé les données personnelles de 147 millions de consommateurs. Equifax a été initialement piraté par le biais d'un portail web de plaintes de consommateurs. Les pirates ont exploité une faille de sécurité qui leur a permis d'obtenir des noms d'utilisateur et des mots de passe pour accéder à d'autres systèmes et extraire des données du réseau.[37]

De plus en plus, les acteurs de la menace obtiennent un accès par le biais de ***l'ingénierie sociale***, en convainquant des initiés de permettre involontairement des intrusions. La forme la plus courante d'ingénierie sociale est ***l'hameçonnage***, dans lequel l'auteur de l'attaque se déguise en partie de confiance (y compris ***l'harponnage***, qui est ciblé et personnalisé pour des initiés individuels).[38] Une étude a révélé que l'ingénierie sociale était utilisée pour soutenir l'infiltration dans 92 % des violations de données en 2020.[39]

Dans une attaque par ***déni de service distribué (DSD)***, l'acteur de la menace obtient un accès non autorisé à des ordinateurs tiers. Il réquisitionne ensuite les systèmes compromis, en les utilisant comme ***zombies*** ou ***bots***, pour lancer une attaque sur la ressource réseau ciblée. En libérant un flot de messages entrants ou de demandes de connexion vers le système ciblé, l'acteur de la menace le force à ralentir ou à tomber en panne, empêchant ainsi les utilisateurs ou les systèmes légitimes de bénéficier du service.[40] Les attaques DSD ont souvent des motivations non financières.

Une fois qu'ils ont obtenu l'accès, les acteurs de la menace utilisent généralement des ***maliciels*** (logiciels malveillants utilisés pour extraire des informations) et peuvent retirer des fonds ou demander le paiement d'une rançon (à l'aide de logiciels malveillants connus sous le nom de ***ransomware***). L'Agence de l'Union européenne pour la cybersécurité (ENISA) a indiqué que les logiciels malveillants constituaient la principale menace de cybersécurité en Europe de janvier 2019 à avril 2020.[41] Une étude a révélé que les logiciels malveillants étaient employés pour localiser, accéder et capturer des données dans la majorité des violations de données de 2020.[42] La même étude a révélé que le piratage par déni de service était impliqué dans près de 60 % des incidents de sécurité.[43]

Contre-mesures publiques et privées pour renforcer la cybersécurité

Le renforcement de la cybersécurité nécessite une action coordonnée des institutions internationales, des gouvernements, des entreprises, de la société civile et des particuliers.

Coopération et coordination internationales

La longue portée et le rythme rapide de l'écosystème numérique transcendent les frontières et permettent aux mauvais acteurs d'agir de manière anonyme et rapide, ce qui a un impact négatif sur de vastes pans de l'humanité.[44] Les institutions internationales interviennent pour faciliter la coopération en matière de cybersécurité. L'ONU a abordé le sujet pour la première fois lors du Sommet mondial sur la société de l'information (SMSI), qui s'est tenu à Genève en 2003 et à Tunis en 2005.[45] Ces sommets visaient à accroître l'accès à Internet dans les pays en développement, à développer une culture mondiale de la cybersécurité et à renforcer la coopération entre les pays relatice à la cybercriminalité.[46] Au sommet de Genève de 2003, l'Union internationale des télécommunications (UIT) a été désignée comme facilitateur des actions du SMSI en matière de cybersécurité afin d'instaurer la confiance et la sécurité dans l'utilisation des Technologies de l'information et de la communication.[47] L'UIT a mis en place un programme de cybersécurité qui offre aux pays en développement un soutien au renforcement des capacités.[48] Le Centre des Nations Unies pour la lutte contre le terrorisme a également mis en place un programme de cybersécurité.[49]

Initiatives des gouvernements nationaux en matière de cybersécurité

Les technologies numériques ont perturbé les cadres de sécurité publique existants, qui ne sont souvent pas adaptés à la protection contre les cyberattaques. Des réformes juridiques et politiques et des activités de mise en œuvre sont nécessaires dans tous les pays pour relever les défis toujours plus grands de la cybersécurité.

Une stratégie nationale de cybersécurité

Face à ces défis, de nombreux gouvernements ont adopté une ***stratégie nationale de cybersécurité***, qui est un plan d'action visant à améliorer la sécurité et la résilience des infrastructures et services nationaux. Ces stratégies reflètent des approches de haut niveau et descendantes de la cybersécurité qui établissent des objectifs, des priorités et des calendriers nationaux.

La première stratégie nationale de cybersécurité, la National Strategy to Secure Cyberspace du gouvernement américain, a été publiée en février 2003 après les attaques terroristes du 11 septembre 2001 contre le World Trade Center.[50] Des plans de cybersécurité plus limités ont été adoptés en Allemagne et en Suède en 2005 et 2006. La deuxième grande stratégie nationale de cybersécurité au monde a été publiée par l'Estonie en 2008, après une grave cyberattaque en 2007.[51]

L'approche consistant à adopter des stratégies nationales a maintenant gagné en popularité. L'Agence de l'Union européenne pour la cybersécurité (ENISA) recommande des stratégies de cybersécurité à tous les États membres de l'UE depuis 2012lii et tient à jour de nombreuses ressources documentaires sur les stratégies nationales de cybersécurité.[53] En 2018, l'UIT a copublié un Guide pour l'élaboration d'une stratégie nationale de cybersécurité avec la Banque mondiale et d'autres institutions.[54] Au moins 114 pays ont adopté ou sont en train d'adopter une stratégie nationale de cybersécurité, dont 17 en Afrique subsaharienne, 18 dans les Amériques, 11 dans les États arabes, 21 dans la région Asie-Pacifique, 6 dans la Communauté des États indépendants et 41 en Europe.[55]

Une agence dédiée à la cybersécurité

De nombreux pays ont créé des agences nationales de cybersécurité autonomes pour assurer le leadership. Ces agences peuvent diriger l'élaboration de la politique de cybersécurité et coordonner sa mise en œuvre dans tous les secteurs. Elles peuvent également servir de porte-parole officiel du gouvernement et de point de contact en cas d'incidents de cybersécurité. Sur la base des données de 198 économies, la Banque mondiale a récemment constaté que des agences de cybersécurité autonomes avaient été créées dans 86 % des pays à revenu élevé, 65 % des pays à revenu moyen supérieur, 66 % des pays à revenu moyen inférieur et 24 % des pays à faible revenu.[56]

Équipes de réponse aux incidents nationales, régionales et sectorielles

Pour se préparer aux incidents de sécurité, les organisations ont mis en place des ***équipes d'intervention en cas d'incident de sécurité informatique (Computer Security Incident Response Teams, ou CSIRT)***, également connues sous le nom ***Computer Emergency Response Team (CERT)***.[57] Pour coordonner les mesures préventives et les interventions en cas d'incident sur le territoire national, les gouvernements ont créé ou désigné des ***CSIRT nationaux (nCSIRT)*** dotés de responsabilités spécifiques en matière de cybersécurité.

Étant donné qu'il est extérieur à sa circonscription, un nCSIRT n'a généralement qu'une autorité limitée pour accéder ou mettre en œuvre des mesures de sécurité au sein des actifs informationnels et technologiques de ses mandants. Elle se concentre sur la coordination de la réponse, l'analyse des menaces et des incidents, et d'autres formes de soutien.[58] L'ONU a recommandé aux pays membres de créer des nCSIRT et de soutenir et faciliter la coopération entre les nCSIRT par-delà les frontières.[59] L'UIT a réalisé des évaluations de nCSIRT pour 79 pays, a aidé 14 pays à créer ou à améliorer leur nCSIRT, et a confirmé qu'au moins 118 pays avaient créé des nCSIRT en mars 2019.[60]

Certaines nCSIRT se sont regroupées au niveau régional pour renforcer leurs efforts face aux cyberattaques transfrontalières, comme l'Asia Pacific Computer Emergency Response Team (APCERT), qui comprend 33 nCSIRT de 23 économies de la région.[61] D'autres organisations similaires comprennent AfricaCERT, avec des nCSIRTs et d'autres membres dans 26 pays africains,[62] et OIC-CERT, sous la responsabilité de l'Organisation de la coopération islamique, avec des nCSIRTs et d'autres membres dans 30 pays.[63] L'ENISA soutient la coopération entre les CSIRTs européens.[64]

Dans certaines industries, les CSIRT sectoriels permettent aux parties prenantes des secteurs public et privé d'unir leurs forces pour faire face aux risques, menaces et autres défis propres à un secteur particulier.[65] L'un des principaux objectifs des CSIRT sectoriels est de protéger les infrastructures critiques essentielles au fonctionnement de la société et de l'économie et de protéger la sécurité nationale. L'infrastructure critique d'un pays peut comprendre les actifs informatiques et technologiques utilisés pour l'énergie, les transports, la finance, la banque, les soins de santé, l'alimentation, l'eau, d'autres chaînes d'approvisionnement essentielles et les activités gouvernementales critiques. Le département de la Sécurité intérieure des États-Unis (US DHS) a identifié 16 secteurs pour les infrastructures critiques.[66] En vertu des lois nationales, les exploitants d'infrastructures critiques peuvent être légalement tenus de se conformer à des

normes et procédures de sécurité renforcées et d'établir des plans de reprise après incident pour atténuer les dommages et favoriser la résilience après un incident de cybersécurité. Ces activités peuvent être coordonnées par une CSIRT sectorielle. L'US DHS continue de surveiller et de mettre à jour les lois et les règlements lorsqu'il constate des lacunes dans le cadre juridique existant. Par exemple, lorsque le Colonial Pipeline a été piraté, l'US DHS a publié deux directives de cybersécurité régissant les pipelines.[67]

La coopération et la coordination se font également entre les CSIRT nationaux, les CSIRT sectoriels et les CSIRT d'entreprises individuelles au niveau international par le biais du Forum of Incident Response and Security Teams (FIRST). Le FIRST compte actuellement 585 CSIRT dans 98 pays.[68]

Mise à jour des lois pénales et des capacités d'application de la loi

L'élaboration de lois pénales et de capacités de répression adaptées est essentielle aux efforts de cybersécurité. La mise à jour du droit pénal matériel est nécessaire lorsque les lois pénales existantes ne couvrent pas les actes commis dans l'écosystème numérique.[69] De nombreux gouvernements ont commencé à analyser et à mettre à jour les lois nationales pour combler les lacunes. Les infractions courantes qui peuvent être ajoutées sont les suivantes :

- Accès non autorisé à des informations ou à des actifs technologiques (piratage),
- Surveillance non autorisée des communications,
- Interception ou l'altération non autorisée d'actifs informationnels,
- Interférence non autorisée avec un système d'information, et
- Utilisation abusive de dispositifs et de logiciels.[70]

Les lois sur la cybercriminalité peuvent également traiter de crimes plus traditionnels, tels que la fraude, la falsification et la violation de la propriété intellectuelle, lorsqu'ils se produisent dans l'écosystème numérique.[71] De nouvelles restrictions sur les contenus en ligne (tels que la pornographie enfantine) ou les comportements en ligne (tels que le cyberharcèlement ou la cyberintimidation) ont également été ajoutées.[72]

Les services répressifs ont également besoin de nouvelles procédures pénales, de nouveaux pouvoirs et de nouveaux outils pour enquêter sur la cybercriminalité et engager des poursuites. Les services répressifs ont également besoin de nouvelles procédures pénales, de nouveaux pouvoirs et de nouveaux outils pour enquêter sur la cybercriminalité et engager des poursuites. Il s'agit notamment de capacités d'expertise informatique dans le cadre des enquêtes, de procédures de conservation et de saisie des preuves électroniques et de mécanismes visant à promouvoir la coopération du secteur privé dans l'identification des menaces et les enquêtes.[73]

L'application de la loi contre la cybercriminalité est également confrontée à des défis juridictionnels en raison de sa nature intrinsèquement sans frontières.[74] Les auteurs peuvent agir rapidement et depuis n'importe quel endroit, en utilisant des actifs technologiques tiers compromis pour masquer leur identité. Par exemple, l'attaque par ransomware WannaCry de 2017 a touché 200 000 ordinateurs dans 150 pays.[75] Une approche harmonisée de la législation et de l'application de la cybercriminalité peut faciliter les efforts d'enquête et d'application entre les juridictions.

La Convention sur la cybercriminalité du Conseil de l'Europe, entrée en vigueur en 2004 et connue sous le nom de Convention de Budapest, est le seul traité international contraignant sur les crimes commis via Internet et d'autres réseaux informatiques.[76] Son principal objectif est de mener une politique pénale commune contre la cybercriminalité en adoptant une législation appropriée et en favorisant la coopération internationale. Il traite des violations de la sécurité des réseaux, de la fraude informatique, de la violation des droits d'auteur et de la pornographie enfantine. Il définit également les pouvoirs et les procédures permettant aux fonctionnaires de fouiller les réseaux informatiques et d'intercepter les communications. Conçue à l'origine comme un traité européen, la Convention de Budapest a été rejointe par 45 des 47 États membres du Conseil de l'Europe et 22 États non membres d'Afrique, des Amériques et d'Asie-Pacifique.[77] Elle reste ouverte à l'adhésion d'autres États.

L'Union africaine a adopté une convention sur la cybersécurité et la protection des données personnelles en juin 2014. Elle n'entrera pas en vigueur tant qu'elle n'aura pas été ratifiée par 15 pays ou qu'elle n'y aura pas adhéré, et elle n'a été signée que par 14 pays et ratifiée par 8.[78] Entre-temps, six pays africains ont adhéré à la Convention de Budapest. L'Organisation des États Américains (OEA) n'a pas adopté de traité sur la cybersécurité. Elle s'occupe de la cybersécurité dans les Amériques par l'intermédiaire du Comité interaméricain contre le terrorisme (CICTE), d'un programme de cybersécurité, et par le biais d'une assistance et d'une formation techniques, de tables rondes politiques, d'exercices de gestion de crise et d'échanges de bonnes pratiques.[79] Dix membres de l'OEA ont adhéré à la Convention de Budapest. L'Association des nations de l'Asie du Sud-Est (ASEAN) n'a pas non plus adopté de traité sur la cybersécurité. En avril 2018, les chefs d'état ont publié une déclaration sur la coopération en matière de cybersécurité.[80] Un membre de l'ASEAN, les Philippines, a adhéré à la Convention de Budapest.

En décembre 2016, quelque 132 pays suivaient le modèle de la Convention de Budapest, dont les 67 parties au traitél.[81]

Le rôle du secteur privé dans la cybersécurité

Pour réussir, les efforts déployés par les gouvernements pour améliorer la cybersécurité doivent s'appuyer sur un écosystème solide et dynamique. Dans les systèmes basés sur le marché de nombreuses économies nationales, la responsabilité de la cybersécurité incombe en grande partie aux entreprises publiques et privées. La plupart d'entre elles ont tout intérêt - et des obligations contractuelles et légales - à adopter et à mettre en œuvre des procédures et des pratiques de sécurité raisonnables. Les administrateurs et les dirigeants ont le devoir, vis-à-vis des créanciers et des actionnaires, de préserver et de protéger les actifs de l'entreprise et de faire preuve de la diligence requise pour sécuriser les actifs informationnels et technologiques. De nombreuses entreprises ont désormais un ***Responsable de la sécurité des systèmes d'information (RSSI)***.[82]

Divers organismes de normalisation nationaux et internationaux ont élaboré des ***cadres de gestion des cyber-risques*** pour guider les entreprises dans la sécurisation des actifs informationnels et technologiques.[83] Ces cadres prescrivent des processus permettant aux entreprises d'identifier leurs actifs informationnels et

technologiques, d'identifier les menaces et les vulnérabilités de ces actifs, d'évaluer le risque de perte (en fonction de la probabilité et de l'impact) et de prescrire des contrôles de sécurité pour réduire le risque à un niveau acceptable. Les ***contrôles de sécurité*** comprennent des mesures de gestion, opérationnelles et techniques visant à protéger la confidentialité, la disponibilité et l'intégrité des actifs informationnels et technologiques. Dans tous les cadres, la gestion des risques est itérative et évolutive.

Les entreprises individuelles créent également de plus en plus leurs propres CSIRT internes pour fournir des services et un soutien à l'entreprise dans l'évaluation, la gestion et la prévention des cyberattaques et la coordination des réponses aux incidents. Ces équipes internes ont un mandat clair et les connaissances nécessaires pour mener des activités pratiques de gestion des incidents au sein des actifs informationnels et technologiques d'une organisation.[84]

Éducation, soutien et ressources en matière de cybersécurité

Les humains sont le maillon faible de la cybersécurité,[85] aussi la sensibilisation et l'éducation du public sont-elles des éléments essentiels d'une cybersécurité efficace. Les entreprises publiques ou privées ont de bonnes raisons de dispenser une formation de sensibilisation à la sécurité à leurs employés : prévenir les incidents de sécurité, construire une culture de la sécurité, renforcer les défenses technologiques, inspirer confiance aux clients, assurer la conformité, être socialement responsable et améliorer le bien-être des employés.[86] Pourtant, de nombreuses entreprises continuent de sous-investir dans la formation. Une enquête menée en 2020 auprès de 3 500 travailleurs en Australie, en France, en Allemagne, au Japon, en Espagne, au Royaume-Uni et aux États-Unis a révélé que beaucoup d'entre eux ne connaissaient toujours pas les meilleures pratiques fondamentales.[87] Les gouvernements et les entreprises ont également de bonnes raisons de sensibiliser et d'éduquer davantage les consommateurs à la cybersécurité. Les entreprises privées considèrent de plus en plus qu'éduquer les consommateurs est une bonne affaire.[88]

Le renforcement des capacités est également vital. Une étude de 2019 a révélé un déficit mondial de compétences de 4 millions de professionnels de la cybersécurité par rapport aux besoins.[89] Les pays développés soutiennent des programmes de formation par le biais d'universités publiques et privées. Par exemple, le National Institute of Standards and Technology des États-Unis a mis en place une initiative visant à faire progresser un écosystème intégré d'éducation, de formation et de développement de la main-d'œuvre en matière de cybersécurité.[90] De même, le gouvernement australien a créé et financé des centres académiques d'excellence en cybersécurité dans deux universités afin d'encourager les étudiants à étudier la cybersécurité et d'augmenter le nombre de diplômés en cybersécurité.[91] L'ENISA envisage des efforts similaires.[92] Les gouvernements des pays en développement ne disposent souvent pas de ressources financières suffisantes pour soutenir le développement des capacités en matière de cybersécurité de manière globale. Toutefois, des pays en développement tels que l'île Maurice et l'Égypte ont fait preuve d'un niveau élevé d'engagement en faveur de la mise en place d'un cadre de cybersécurité solide, comme en témoigne l'indice mondial de cybersécurité (Global Cybersecurity Index, ou GCI).[93] L'UIT a également apporté un soutien technique important aux

CSIRT, mais la communauté internationale n'a pas encore fourni de financement suffisant pour former des professionnels de la cybersécurité dans les pays en développement.[94]

Questions émergentes

Le travail à domicile entraîne de nouvelles vulnérabilités

La pandémie de COVID-19 et les confinements qui en ont résulté ont changé la façon dont de nombreuses personnes effectuent des activités de base telles que travailler, faire les courses et aller à l'école. Le passage du travail dans un bureau au travail à distance depuis la maison a introduit et exposé des vulnérabilités en cybersécurité. Les ordinateurs domestiques sont souvent dépourvus des protocoles de sécurité que l'on trouve au bureau. Les entreprises qui font appel à des fournisseurs tiers pour surveiller et traiter les cybermenaces peuvent constater que ces solutions ne s'appliquent pas de manière transparente au travail à distance.

Les cybercriminels ont exploité ces lacunes. Le FBI (Federal Bureau of Investigation américain) a signalé que le nombre de plaintes pour cyberattaques en 2020 a augmenté de 400 % par rapport aux taux antérieurs à la COVID, atteignant jusqu'à 4 000 par jour. Un fournisseur de cybersécurité a signalé plus d'attaques sur les réseaux d'entreprise au premier semestre 2020 que sur l'ensemble de l'année 2019.[95] L'utilisation de ransomwares a augmenté de manière significative.[96] Ces nouvelles vulnérabilités exigeront que les entreprises et autres organisations s'adaptent et éduquent les employés sur la manière d'éviter et de minimiser les menaces lorsqu'ils travaillent à distance.[97]

Blockchains et crypto-monnaies

Une ***blockchain*** est un type de base de données qui utilise la ***technologie du registre distribué (TRD)***, une infrastructure de réseau décentralisée qui permet l'accès, la validation et la mise à jour simultanés des enregistrements de manière immuable dans plusieurs endroits.[98] En éliminant le besoin d'une autorité centralisée, la blockchain est potentiellement plus résistante à la falsification, ce qui favorise la confiance et en fait une technologie de cybersécurité potentiellement utile et solide.

La ***crypto-monnaie*** est une forme de monnaie numérique qui s'appuie sur la technologie blockchain pour suivre la valeur et enregistrer les transactions sans aucune autorité de compensation. La cryptographie permet aux participants aux transactions de rester anonymes. Les échanges de crypto-monnaies font face à une réglementation potentielle pour empêcher le blanchiment d'argent et d'autres activités illégales et pour s'assurer que les traders déclarent leurs bénéfices et paient des impôts aux autorités. Mais jusqu'à présent, la loi n'a pas suivi et les crypto-monnaies et les transactions dans ces monnaies sont largement non réglementées. Elles sont devenues un moyen de paiement privilégié pour les cybercriminels. Les experts du secteur pensent que cela a contribué à une augmentation de 311 % des paiements de ransomware entre 2019 et 2020.[99]

Les ***monnaies numériques des banques centrales (MNBC)*** sont un autre type de monnaie numérique qui s'appuie sur la DLT, mais qui est émise par la banque centrale d'une nation, comme l'émission de la monnaie papier. En raison de la sécurité et de la fiabilité de la DLT sous-jacente, les MNBC pourraient réduire le coût et accroître l'efficacité des transactions, en permettant le règlement immédiat de

transactions qui prenaient auparavant plusieurs jours. Contrairement aux crypto-monnaies, les MNBC ne sont pas censées être anonymes, et l'enregistrement immuable des transactions créé par la TRD soulève des préoccupations potentielles de la confidentialité. En octobre 2020, les Bahamas ont lancé la première MNBC au monde, connue sous le nom de Sand Dollar. Un an après le lancement, l'utilisation était encore faible, mais des efforts accrus d'éducation et de sensibilisation du public étaient prévus.

Ressources supplémentaires

Cadres modèles de cybersécurité

- Département américain de la sécurité intérieure, stratégie de cybersécurité, 2018
- Stratégie australienne de cybersécurité 2020 (anglais)
- Convention de Budapest sur la cybercriminalité
- Loi sur la cybersécurité de l'UE

Pour en savoir plus

- Recommendation of the Council on Digital Security of Critical Activities (anglais), OECD, 2021
- Cybersecurity Policy Framework, A practical guide to the development of national cybersecurity policy (anglais), Microsoft, 2018
- Guide to Developing a National Cybersecurity Strategy (anglais), ITU, 2017
- Combatting Cybercrime, Tools and Capacity Building for Emerging Economies (anglais) Banque Mondiale, 2017

Organisations

- Direction de la Société de l'information et de l'action contre la criminalité
- Cybersecurity & Infrastructure Security Agency (CISA)
- ITU (Page cybersécurité)
- National Cybersecurity Alliance
- United States Department of Homeland Security (Page cybersécurité)
- L'Agence de l'Union européenne pour la cybersécurité (ENISA)
- Payment Card Industry Security Standards Council
- Cloud Security Alliance
- McAfee Resource Library
- Microsoft Cybersecurity
- Cybercrime Magazine

Notes

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[2] La sécurité des données est le processus de maintien de la confidentialité, de l'intégrité et de la disponibilité des données d'une organisation d'une manière compatible avec la stratégie de risque de l'organisation. https://www.nccoe.nist.gov/data-security

[3] Prévention des dommages, protection et restauration des ordinateurs, des systèmes de communications électroniques, des services de communications électroniques, des communications par fil et des communications électroniques, y compris les informations qu'ils contiennent, afin de garantir leur disponibilité, leur intégrité, leur authentification, leur confidentialité et leur non-répudiation. https://csrc.nist.gov/glossary/term/cybersecurity

[4] Voir, par exemple, Richard A. Caralli, James F. Stevens, Lisa R. Young et William R. Wilson, Software Engineering Institute, Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process, Technical Report CMU/SEI-2007-TR-012, Appendix A, Step 2 at 34-35 (mai 2007) [le rapport technique OCTAVE Allegro]. Disponible à l'adresse https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.

[5] Voir, par exemple, le rapport technique d'OCTAVE Allegro, supra, aux pages 34 et 35.

[6] Voir, par exemple, le rapport technique d'OCTAVE Allegro, supra, §2.4.2.2 à 12 et l'annexe A, étape 2 à 34.

[7] Les trois éléments de sécurité de l'information que sont la confidentialité, l'intégrité et la disponibilité ont été formulés pour la première fois dans le compte rendu d'un atelier organisé en mars 1977 par le US Institute for Computer Sciences and Technology. Voir Zella G. Ruthberg, ed., Institute for Computer Sciences and Technology, National Bureau of Standards, Computer Science & Technology : Audit and Evaluation of Computer Security, Proceedings of the NBS Invitational Workshop held at Miami Beach, Florida, March 22-24, 1977 at xxii (Oct 1977) (identifiant "trois composantes vitales de l'audit - contrôle d'accès, précision et disponibilité"). Disponible à l'adresse https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf. Ces trois composantes sont toujours considérées comme les objectifs fondamentaux de la sécurité de l'information. Voir, par exemple, Center for Internet Security, "EI-ISAC Cybersecurity Spotlight - CIA Triad" (2021). Disponible à l'adresse https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/.

[8] Un individu ou un groupe qui représente une menace. https://csrc.nist.gov/glossary/term/threat_actor

[9] La première cyberattaque connue a eu lieu en novembre 1988, lorsque Robert Morris, étudiant diplômé, a diffusé un ver informatique malveillant, connu sous le nom de ver Morris, à partir d'un ordinateur du MIT qu'il avait piraté (auquel il avait accédé sans autorisation) depuis son terminal sur le système informatique de l'université Cornell. Le ver s'est copié d'ordinateur en ordinateur, épuisant les ressources du système. L'incident s'est produit avant l'introduction du web mondial, lorsque l'Internet était encore dominé par les utilisateurs militaires et universitaires. En 24 heures, 6 000 des 60 000 ordinateurs de l'Internet ont été désactivés.

[10] Voir, par exemple, Michelle Drolet, "The Evolving Threat Landscape : Five Trends to Expect In 2020 And Beyond", Forbes (14 janvier 2020). Disponible à l'adresse https://www.forbes.com/sites/forbestechcouncil/2020/01/14/the-evolving-threat-landscape-five-trends-to-expect-in-2020-and-beyond/?sh=23d52320521d.

[11] Le volume annuel de données créées, capturées, copiées et consommées dans le monde a augmenté de plus de 3 000 %, passant de 2 zettaoctets en 2010 à 64,2 zettaoctets en 2020. Arne Holst, "Volume de données/informations créées, capturées, copiées et consommées dans le monde de 2010 à 2025" (Statistica, 7 juin 2021) Disponible à l'adresse suivante https://www.statista.com/statistics/871513/worldwide-data-created/.

[12] Equinix, le leader mondial des centres de données, prévoit que d'ici 2023, les entreprises atteindront des taux de croissance annuels de 50 % de la bande passante nécessaire à l'interconnexion avec les fournisseurs et les clients. Equinix, Global Interconnection Index Volume 4 (2020). Disponible à l'adresse https://www.equinix.com/gxi-report#forecast.

[13] TLe marché mondial de la synchronisation et du partage de documents, photos, vidéos et fichiers en entreprise devrait passer de 4,23 milliards USD en 2019 à 16,99 milliards USD en 2025. Voir ReportLinker, Enterprise File Synchronization and Sharing (EFSS) Market - Growth, Trends, Forecasts (2020 - 2025) (mai 2020). Disponible à l'adresse https://www.reportlinker.com/p05865744/Enterprise-File-Synchronization-and-Sharing-Market-EFSS-Growth-Trends-and-Forecast.html.

[14] En janvier 2021, Facebook comptait plus de 2,6 milliards d'utilisateurs mensuels actifs, dont 80 % accédaient à leur compte exclusivement à partir d'appareils mobiles. H. Tankovska, "Countries with the most Facebook users 2021", Statistica (9 février 2021). Disponible à l'adresse https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.

[15] À la mi-2020, plus de 850 millions de comptes d'argent mobile avaient été ouverts dans 90 pays, et une moyenne de 1,3 milliard USD par jour était transigée sur ces comptes. Ceyla Pazarbasioglu & Alfonso Garcia Mora, "Expanding digital financial services can help developing economies cope with crisis now and boost growth later," World Bank Blogs (29 Apr 2020). Disponible à l'adresse https://blogs.worldbank.org/voices/expanding-digital-financial-services-can-help-developing-economies-cope-crisis-now-and-boost-growth-later.

[16] Thomas Alsop, "Computer penetration rate among households in developing countries 2005-2019", Statistica (18 février 2021). Disponible à l'adresse https://www.statista.com/statistics/748564/developing-countries-households-with-computer/.

[17] https://data.worldbank.org/indicator/IT.CEL.SETS.P2

[18] GSMA, Rapport sur l'état de l'industrie de l'argent mobile 2021 (2021). Disponible à l'adresse https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money-2021_Full-report.pdf.

[19] Silvia Baur-Yazbeck, " Les cyberattaques constituent un problème croissant dans les pays en développement ", Opinion, Inter Press Service News Agency (8 octobre 2018). Disponible à l'adresse http://www.ipsnews.net/2018/10/cyber-attacks-growing-problem-developing-nations/

[20] Kshetri, Nir, " Cybercrime et cybersécurité en Afrique ", Journal of Global Information Technology Management, vol. 22, n°2, 77-81 (2019). Disponible à l'adresse suivante https://doi.org/10.1080/1097198X.2019.1603527.

[21] Business Ghana, " La Banque du Ghana lance une directive sur la cybersécurité pour les institutions financières ", (25 octobre 2018). Disponible à l'adresse suivante https://www.businessghana.com/site/news/business/175019/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions.

[22] Les systèmes numériques de contrôle de supervision et d'acquisition de données (SCADA) sont utilisés dans tous les pays en développement, sauf les plus petits, pour surveiller et gérer les réseaux électriques. Varun Nangia, Samuel Oguah & Kwawu Gaba, "Managing the Grids of the Future in Developing Countries : Recent World Bank Support for SCADA/EMS and SCADA/DMS Systems ", LiveWire (World Bank Group 2016). Disponible à l'adresse https://openknowledge.worldbank.org/handle/10986/24717; et Tal Avrahami, " SCADA pour la surveillance à distance des services publics : 4 Layers to Grasp ", IIoT World (23 mars 2017). Disponible à l'adresse https://iiot-world.com/industrial-iot/connected-industry/scada-systems-for-remote-utilities-monitoring-the-four-layers-you-need-to-understand/.

[23] La protection de ces informations et de ces actifs technologiques est vitale pour une distribution sûre et fiable de l'électricité. Le Conseil mondial de l'énergie a constaté une augmentation de 87 attaques en 2014 à 150 en 2019, et 80 % des entreprises du secteur de l'énergie ne sont pas préparées à gérer les cyberattaques. Power Africa, "Cybersécurité pour la transmission et la distribution en Afrique" (20 juillet 2020). Disponible à l'adresse https://powerafrica.medium.com/cybersecurity-for-transmission-and-distribution-in-africa-475676074534.

[24] Le réseau électrique ukrainien à nouveau piraté, un signe inquiétant pour les attaques contre les infrastructures (Déc 2016). Disponible à l'adresse https://www.technologyreview.com/2016/12/22/5969/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

[25] " Une cyberattaque coupe le réseau de l'autorité municipale de Johannesburg ", Reuters 25 octobre 2019). Disponible sur https://www.reuters.com/article/us-safrica-crime/cyber-attack-shuts-johannesburg-city-authoritys-network-idUSKBN1X41RF.

[26] Les coûts directs à l'échelle mondiale en 2020 étaient en hausse par rapport à 522,5 milliards USD en 2018, 475 milliards USD en 2014 et 300 milliards USD en 2013. Zhanna Malekos Smith & Eugenia Lostri, McAfee et le Center for Strategic and International Studies & McAfee, The Hidden Costs of Cybercrime, Report (7 déc. 2020) [le "Rapport McAfee 2020"]. Disponible à l'adresse https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

[27] Voir le rapport McAfee 2020, précité.

[28] Le PIB mondial en 2020 a été estimé à 84,54 trillions USD. Aaron O'Neill, Statistica, Global gross domestic product (GDP) at current prices from 1985 to 2026 (1 Jun 2021). Disponible à l'adresse https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/.

[29] " Le coût de la cybercriminalité ", The Economist (22 juin 2018). Disponible à l'adresse https://www.eiu.com/industry/article/1586874742/the-cost-of-cyber-crime/2018-06-22.

[30] Paul Dreyer et al, Estimation du coût mondial du cyber-risque : méthodologie et exemples à ix (2018). Disponible à l'adresse https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf.

[31] Voir Steve Morgan, "McAfee Vastly Underestimates the Cost of Cybercrime", Cybercrime Magazine (9 décembre 2020). Disponible à l'adresse https://cybersecurityventures.com/mcafee-vastly-underestimates-the-cost-of-cybercrime/.

[32] La banque centrale du Bangladesh détenait ses réserves de devises auprès de la Federal Reserve Bank of New York. Malgré les avertissements du système de transfert interbancaire SWIFT, la banque centrale n'avait pas séparé son serveur SWIFT de son réseau informatique. Fin 2015, des intrus se sont introduits à distance dans le réseau informatique de la banque et ont installé un logiciel malveillant. Le 4 février 2016, au moment de la fermeture des banques, ils ont émis 70 instructions de paiement pour transférer 1 milliard de dollars de fonds de la banque vers de faux comptes aux Philippines et au Sri Lanka. La surveillance humaine a bloqué certains paiements, mais 81 millions USD ont été envoyés sur des comptes frauduleux et blanchis par le système de casino philippin. Joshua Hammer, "The Billion-Dollar Bank Job", The New York Times (3 mai 2018). Disponible à l'adresse suivante www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

[33] Une enquête menée en 2021 a analysé 29 207 incidents de sécurité dans 88 pays, dont 5 258 violations de données, signalés en 2020. Verizon, 2021 Data Breach Investigations Report at 6, 12 & 14 (2021) [le DBIR de Verizon 2021]. Disponible à l'adresse https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

[34] "Les hacktivistes de WikiLeaks font tomber MasterCard", Finextra (28 juin 2011). Disponible sur https://www.finextra.com/newsarticle/22713/wikileaks-hacktivists-take-down-mastercard.

[35] Voir, par exemple , Lyndon Sutherland, " Know Your Enemy : Understanding the Motivation Behind Cyberattacks ", SecurityIntelligence (31 mars 2016). Disponible à l'adresse https://securityintelligence.com/know-your-enemy-understanding-the-motivation-behind-cyberattacks/.

[36] La liste des cyberincidents importants depuis 2006, compilée par le Center for Strategic & International Studies, révèle de multiples cyberattaques qui auraient été menées par des acteurs de la menace parrainés par l'État. Center for Strategic & International Studies, "Significant Cyber Incidents" (mai 2021). Disponible à l'adresse https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[37] Josh Fuhlinger, "Equifax data breach FAQ : Que s'est-il passé, qui a été affecté, quel a été l'impact ? ". CSO (12 février 2020). Disponible à l'adresse https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[38] Cheryl Conley, " Navigating the Phishy Social Engineering Ocean ", SANS Institute Blog (27 juin 2019). Disponible à l'adresse https://www.sans.org/blog/navigating-the-phishy-social-engineering-ocean/.

[39] Verizon, 2021 Data Breach Investigations Report, p. 6, 12 et 14 (2021) [le DBIR de Verizon 2021]. Disponible à l'adresse https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

[40] Voir Agence américaine de cybersécurité et de sécurité des infrastructures, Conseil de sécurité (ST04-015) : Comprendre les attaques par déni de service (mis à jour le 20 novembre 2019). Disponible à l'adresse https://us-cert.cisa.gov/ncas/tips/ST04-015.

[41] ENISA, De janvier 2019 à avril 2020, l'année en revue : Le paysage des menaces de l'ENISA à 11 ans (20 Oct 2020)[Revue ENISA 2020]. Disponible à l'adresse https://www.enisa.europa.eu/publications/year-in-review.

[42] Verizon 2021 DBIR, supra, p. 17.

[43] Verizon 2021 DBIR, supra, p. 15.

[44] Voir, par exemple, Chuck Brooks, "Alarming Cybersecurity Stats : What You Need to Know For 2021", Forbes (2 mars 2021). Disponible à l'adresse https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=c0017958d3df.

[45] Voir, par exemple, Nations Unies, Département des affaires économiques et sociales, Institutions publiques, Sommet mondial sur la société de l'information (SMSI), disponible à l'adresse suivante https://publicadministration.un.org/en/Themes/ICT-for-Development/World-Summit-on-Information-Society.

[46] L'un des principaux objectifs du SMSI était de réduire la fracture numérique mondiale en améliorant l'accès à l'internet dans les pays en développement. L'agenda de Tunis a réaffirmé la nécessité de développer une culture mondiale de la cybersécurité par une action nationale et une coopération internationale accrue. Le SMSI a souligné la nécessité de disposer d'outils et d'actions efficaces et efficients, aux niveaux national et international, pour promouvoir la coopération internationale en matière de cybercriminalité. Voir Sommet mondial sur la société de l'information, Agenda de Tunis pour la société de l'information, §39 et §40, WSIS-05/TUNIS/DOC/6(Rev. 1)-F (18 novembre 2005). Disponible à l'adresse https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[47] Voir Alexander Ntoko, Division de la stratégie d'entreprise, UIT, "Global Cybersecurity Agenda : a framework for international cooperation", (Groupe intergouvernemental d'experts à composition non limitée sur la cybercriminalité, Vienne, 17-21 janvier 2011). Disponible à l'adresse https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf

[48] Voir UIT, "Cybersécurité > Mandat" (2021). Disponible à l'adresse https://www.itu.int/en/ITU-D/Cybersecurity/Pages/about-cybersecurity.aspx

[49] Voir Nations unies, Bureau du contre-terrorisme, "What we do > Cybersecurity" (2021). Disponible à l'adresse https://www.un.org/counterterrorism/cybersecurity.

[50] Voir Gouvernement des États-Unis, The National Strategy to Secure Cyberspace (février 2003). Disponible à l'adresse https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[51] Voir ENISA, National Cyber Security Strategies : Setting the course for national efforts to strengthen security in cyberspace §2 (mai 2012)[ENISA Cybersecurity Strategies Paper]. Disponible à l'adresse https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

[52] Voir le document sur les stratégies de cybersécurité de l'ENISA, supra.

[53] Voir, par exemple , ENISA, Bonnes pratiques en matière d'innovation sur la cybersécurité dans le cadre des stratégies nationales de cybersécurité (Nov 2019). Disponible à l'adresse https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

[54] Voir UIT, Banque mondiale, Secrétariat du Commonwealth, Organisation des télécommunications du Commonwealth, OTAN Centre d'excellence en cyberdéfense coopérative, Guide d'élaboration d'une stratégie nationale de cybersécurité - Engagement stratégique en matière de cybersécurité (2018). Disponible à l'adresse suivante https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[55] UIT, Référentiel des stratégies nationales de cybersécurité (2021). Disponible à l'adresse https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[56] Groupe de la Banque mondiale, Data for Better Lives : Rapport sur le développement dans le monde 2021 à 277 (2021). Disponible sur https://www.worldbank.org/en/publication/wdr2021.

[57] Lors de l'incident du ver Morris en novembre 1988, la réponse était isolée, non coordonnée et lente à résoudre l'incident. Par la suite, le ministère américain de la défense a créé un centre de coordination des équipes d'intervention en cas d'urgence informatique au Carnegie Mellon University Software Engineering Institute. Son mandat était d'aider les autres organisations à mettre en place des CSIRT. Voir, US Federal Bureau of Investigation, "The Morris Worm : 30 Years Since First Major Attack on the Internet ", News (2 nov. 2018)(article sur le ver Morris du FBI). Disponible à l'adresse suivante https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

[58] Voir Forum mondial sur la cyber-expertise, Global CSIRT Maturity Framework : Stimuler le développement et l'amélioration de la maturité des CSIRT nationaux à 6 (Version 1.0, juin 2019)[Global CSIRT Maturity Framework]. Disponible à l'adresse https://thegfce.org/wp-content/uploads/2020/05/MaturityFrameworkfornationalCSIRTsv1.0_GFCE.pdf.

[59] Nations unies, Groupe d'experts gouvernementaux sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, Rapport §17(c) & (d) (23 juil. 2015), adopté par l'Assemblée générale dans la résolution A/RES/70/237 (2015). Disponible à l'adresse https://undocs.org/A/70/174.

[60] UIT, UIT-D Cybersécurité > CIRT national (2021). Disponible sur https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[61] L'APCERT a été créé en 2003 par les nCSIRTs et d'autres CSIRTs de 12 pays d'Asie-Pacifique et comprend maintenant des pays allant de Tonga, pour les plus petits, à l'Inde et la Chine, pour les plus grands. Voir Asia Pacific Computer Emergency Response Team, APCERT Annual Report 2020 (27 avril 2021). Disponible à l'adresse http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf.

[62] Voir AfricaCERT, Membership (2021). Disponible à l'adresse https://www.africacert.org/african-csirts/.

[63] Voir OIC-CERT, Liste des membres > Tous les membres (2021). Disponible à l'adresse https://www.oic-cert.org/en/allmembers.html#.YMy0K75KiUk.

[64] Voir ENISA, Topics > CSIRTs and communities (2021). Disponible à l'adresse https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts.

[65] Voir l' institut de génie logiciel de l'université Carnegie Mellon, The Sector CSIRT Framework : Developing Sector-Based Incident Response Capabilities, rapport technique (juin 2021). Disponible à l'adresse https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf.

[66] Agence américaine de cybersécurité et de sécurité des infrastructures, Secteurs d'infrastructures critiques. Élection fédérale L'infrastructure est considérée comme faisant partie du secteur des installations gouvernementales.

[67] https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/

[68] FIRST a été créé en 1985 en tant qu'organisation à but non lucratif par un groupe de CSIRT parties prenantes pour favoriser la coopération et la coordination dans la prévention des incidents, stimuler la réaction rapide aux incidents et promouvoir le partage d'informations entre les membres et la communauté dans son ensemble. Forum of Incident Response and Security Teams, FIRST members around the world (2021). Disponible à l'adresse https://www.first.org/members/map.

[69] Voir, par exemple, UIT, Comprendre la cybercriminalité : Phénomènes, défis et réponse juridique, à 3 (sept 2012). Disponible à l'adresse https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

[70] Voir, de manière générale, Banque mondiale et Nations unies, Combatting Cybercrime : Outils et renforcement des capacités pour les économies émergentes, à 78 (2017). Disponible à l'adresse https://documents1.worldbank.org/curated/en/355401535144740611/pdf/129637-WP-PUBLIC-worldbank-combating-cybercrime-toolkit.pdf

[71] Id.

[72] Id.

[73] Id., p. 95 et 109.

[74] Id. à 121.

[75] Voir Mike Azzara, All You Need to Know about WannaCry Ransomware, Mimecast Blog (5 mai 2021). Disponible à l'adresse https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/.

[76] Voir Conseil de l'Europe, Détails du Traité n° 185, Convention sur la cybercriminalité (entrée en vigueur le 1er juillet 2004). Disponible sur https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[77] Voir Conseil de l'Europe, Tableau des signatures et ratifications du Traité 185, Convention sur la cybercriminalité (état au 15 juin 2021). Disponible sur https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[78] Voir Union africaine, Liste des pays qui ont signé, ratifié ou adhéré à la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (état au 18 juin 2020). Disponible à l'adresse https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[79] Voir OEA, Cyber Security (2021). Disponible à l'adresse https://www.oas.org/en/topics/cyber_security.asp.

[80] Voir la déclaration des dirigeants de l'ASEAN sur la coopération en matière de cybersécurité, 32e sommet de l'ASEA (18 avril 2018). Disponible à l'adresse https://asean.org/storage/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf.

[81] Alexander Seger, Conseil de l'Europe, " Mise en œuvre de la Convention de Budapest sur la cybercriminalité " à la diapositive 3 (Réunion du groupe de travail sur la cybercriminalité, réunions de l'OEA des ministres de la Justice ou des procureurs généraux des Amériques, Washington, DC, 12-13 déc 2016). Disponible à l'adresse suivante . https://www.oas.org/juridico/PDFs/cyb9_coe_cyb_oas_Dec16_v1.pdf.

[82] Voir, par exemple , Nader Mehravari & Julia Allen, " Structuring the Chief Information Security Officer (CISO) Organization ", Carnegie Mellon Software Engineering Institute Blog (22 février 2016). Disponible à l'adresse https://insights.sei.cmu.edu/blog/structuring-chief-information-security-officer-ciso-organization/.

[83] Voir, par exemple : (1) Système de gestion de la sécurité de l'information ISO/IEC 27001 développé par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI). Disponible à l'adresse https://www.iso.org/isoiec-27001-information-security.html. (2) Cadre de cyber-risque "Factor analysis of information risk" (FAIR) développé par l'Open Group. Disponible à l'adresse https://www.opengroup.org/forum/security/riskanalysis. ((3) Cadre de cybersécurité du National Institute of Standards and Technology des États-Unis (NIST CSF). Disponible à l'adresse https://www.nist.gov/cyberframework. (4) Cadre de gestion des risques du ministère américain de la Défense (RMF). Disponible à l'adresse https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=qEE2HGN_HE4Blu7161t1TQ%3D%3D.

[84] Voir le Global CSIRT Maturity Framework, supra

[85] Par exemple, l'erreur humaine a été attribuée à 90 % des cyber-violations de 2019 au Royaume-Uni. CybSafe, " Human error to blame for 9 in 10 UK cyber data breaches in 2019 " (7 février 2020). Disponible à l'adresse https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/.

[86] CybSafe, "7 reasons why security awareness training is important" (26 Jan 2021). Disponible à l'adresse https://www.cybsafe.com/community/blog/7-reasons-why-security-awareness-training-is-important/.

[87] Proofpoint, 2020 User Risk Report : Exploring Vulnerability and Behavior in a People-Centric Threat Landscape, à la page 6 (avril 2020). Disponible à l'adresse https://www.proofpoint.com/sites/default/files/2020-05/gtd-pfpt-us-tr-user-risk-report-2020_0.pdf.

[88] Voir, par exemple, "Eight Ways Companies Can Educate Customers About Cybersecurity Threats", Forbes (30 mars 2021). Disponible à l'adresse https://www.forbes.com/sites/theyec/2021/03/30/eight-ways-companies-can-educate-customers-about-cybersecurity-threats/?sh=5898bc384077

[89] Estimation d'un déficit de main-d'œuvre de plus de 500 000 personnes en Amérique du Nord, 600 000 en Amérique latine, près de 300 000 en Europe et 2,6 millions dans la région Asie-Pacifique. Aucune estimation n'a été fournie pour l'Afrique ou le Moyen-Orient (ISC)2, Strategies for Building and Growing Strong Cybersecurity Teams : (ISC)2 Cybersecurity Workforce Study, 2019 à 8 (2019). Disponible à l'adresse https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.

[90] Voir NIST, National Initiative for Cybersecurity Education (2021). Disponible à l'adresse https://www.nist.gov/itl/applied-cybersecurity/nice.

[91] Voir Gouvernement australien, ministère de l'Énergie, des Sciences, de l'Énergie et des Ressources, "What is the government doing in cyber security ?" (2021). Disponible à l'adresse https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security.

[92] Voir ENISA, Topics > Cybersecurity Education > European Cybersecurity Skills Framework (2021). Disponible à l'adresse https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.

[93] Indice mondial de cybersécurité (ICG) 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[94] Voir, par exemple, Lilly Pijnenburg Muller, Cyber Security Capacity Building in Developing Countries : Challenges and Opportunities at 12, rapport NUPI n° 3 (2015). Disponible à l'adresse https://cybilportal.org/wp-content/uploads/2020/06/NUPIReport03-15-Muller.pdf.

[95] R. Ackerman, "Les entreprises doivent renforcer leur cybersécurité dans la perspective de la poursuite du COVID-19 en 2021," Security Magazine (7 Jan 2021).

[96] D. Nagel, "Le secteur de l'enseignement secondaire est devenu le segment le plus ciblé par les logiciels rançonneurs," The Journal (11 Dec 2020).

[97] Voir R. Ackerman, supra; Chambre de commerce des États-Unis, Special Report on Cybersecure Working During COVID-19 ; M. Castelo, "How School Districts Should Respond to Ransomware Attacks," EdTech Magazine (30 Sep 2020).

[98] Frankenfield, Jake, Investopedia, "Distributed Ledger Technology (DLT)," (27 août 2021). Disponible à l'adresse https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp.

[99] Voir, par exemple, Chris Matthews, "Bitcoin extortion : How cryptocurrency has enabled a massive surge in ransomware attacks", MarketWatch (15 mai 2021). Disponible à l'adresse https://www.marketwatch.com/story/bitcoin-extortion-how-cryptocurrency-has-enabled-a-massive-surge-in-ransomware-attacks-11621022496.

À propos de l'UNCDF

L'UN Capital Development Fund (UNCDF) facilite l'accès aux capitaux publics et privés par les populations les plus démunies dans les 46 pays les moins avancés du monde (PMA).

Dans le cadre de son mandat de fourniture de capitaux et d'instruments d'investissement, l'UNCDF offre des modèles de financement du «last mile» permettant de débloquer les ressources publiques et privées, notamment au niveau national, afin de réduire la pauvreté et d'encourager le développement économique local.

Les modèles de financement de l'UNCDF ouvrent à travers trois axes, à savoir : 1) les économies numériques inclusives, qui connectent les personnes, les ménages et les petites entreprises aux écosystèmes financiers qui catalysent la participation à l'économie locale et fournissent des outils pour vaincre la pauvreté et gérer leur vie financière ; 2) le financement du développement local, qui permet aux municipalités de dynamiser l'expansion économique locale et le développement durable par le biais de la décentralisation fiscale, du financement municipal innovateur et du financement structuré de projets ; et 3) le financement d'investissements, qui fournit une structuration financière catalytique, une réduction des risques et le déploiement des investissements pour favoriser l'impact des ODD et la mobilisation des ressources au niveau national.

L'UNCDF Policy Accelerator travaille avec les gouvernements pour les aider à créer des politiques et des réglementations qui incluent tout le monde dans l'économie numérique, partage des outils et des guides pratiques basés sur notre modèle d'assistance technique et nos ressources de référence, et fourni des bourses aux décideurs politiques et aux régulateurs pour qu'ils puissent étudier avec nos organisations partenaires de classe mondiale.

À propos de Macmillan Keck

Macmillan Keck Attorneys & Solicitors conseille ses clients en matière de stratégie, de plaidoyer, d'affaires controverses et réformes dans l'économie numérique. Les clients du cabinet comprennent des opérateurs de télécom les fournisseurs de services financiers numériques, les fournisseurs de services de santé et d'éducation en ligne fournisseurs de contenu, d'applications et de services numériques, des gouvernements et des autorités de régulation de la concurrence et des organisations internationales. Le cabinet a mené à bien de nombreux projets complexes dans une majorité de pays sur tous les continents.

Clause de non-responsabilité

Les appellations utilisées sur cette carte et la présentation des données qui y figurent n'impliquent aucune prise de position de la part du Secrétariat de l'Organisation des Nations Unies ou de l'UNCDF quant au statut juridique des pays, territoires, villes ou zones.

Cette publication a été révisée pour la dernière fois en Février 2022

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US