JIU/REP/2021/3

Nations Unies

La cybersécurité dans les entités des Nations Unies

Rapport du Corps commun d'inspection

Établi par Jorge Flores Callejas, Aicha Afifi et Nikolay Lozinskiy

JIU/REP/2021/3
Français
Original: anglais

La cybersécurité dans les entités des Nations Unies

Rapport du Corps commun d'inspection

Établi par Jorge Flores Callejas, Aicha Afifi et Nikolay Lozinskiy

Nations Unies • Genève, 2021

Équipe chargée de l'examen

Jorge Flores Callejas, Aicha Afifi et Nikolay Lozinskiy, Inspecteurs

Vincent Hermie, Spécialiste de l'évaluation et de l'inspection

Szilvia Petkov, Spécialiste adjointe de l'évaluation et de l'inspection

Hervé Baudat, Assistant de recherche

Dejan Dincic, Consultant

Charlotte Claveau, Alina Datsii et Bianca Canevari, stagiaires

Résumé analytique

La cybersécurité dans les entités des Nations Unies

Dans notre monde numérisé, la question de la cybersécurité a pris toute son importance pour les organisations internationales. Les entités des Nations Unies n'échappent pas à cette réalité. La transformation numérique, la dépendance croissante à l'égard des technologies de l'information et des communications (TIC), ainsi que des solutions en ligne, et le fait que les menaces à la cybersécurité ne cessent de se faire plus pressantes, tant par leur sophistication que par leur pouvoir de perturbation, ont donné lieu à une augmentation inédite des cyberrisques auxquels sont confrontées les entités des Nations Unies. La cybersécurité est certes née dans la sphère des TIC, mais à présent que les systèmes de gestion de l'information sont profondément implantés dans les activités des entités, que le paysage des menaces a considérablement évolué et que les défenses à caractère technologique ne suffisent plus, il ne semble plus viable de considérer la cybersécurité seulement sous l'angle restrictif des TIC. Dans le présent rapport, les Inspecteurs plaident en faveur de l'intégration des considérations de cybersécurité dans des cadres institutionnels plus larges, tels que la gestion du risque institutionnel, la planification de la continuité des opérations et la sûreté et la sécurité, et ils en préconisent la transversalisation dans toute l'entité.

Il y a eu, ces dernières années, parmi les entités des Nations Unies, une prise de conscience croissante de l'importance à accorder à la cybersécurité. La faiblesse d'un dispositif de sécurité peut en effet avoir des répercussions qui vont au-delà de la perturbation des infrastructures et des systèmes informatiques et de communication, ou encore du volume d'informations compromises. C'est aussi la capacité des entités d'exécuter leur mandat et de maintenir leur crédibilité aux yeux de leurs membres et de leurs bénéficiaires qui sont en jeu. En outre, de nombreuses catégories d'individus dont les données sont détenues par des entités des Nations Unies peuvent se trouver exposés à de graves préjudices en cas de fuite de ces informations. S'il est vrai que les cyberattaques peuvent toucher différemment des entités dont les mandats et les structures diffèrent, la menace qu'elles représentent n'en reste pas moins réelle et partagée. Aucune entité ne sera jamais tout à fait à l'abri d'une atteinte à sa cybersécurité, quel que soit son niveau de préparation et de vigilance, mais celle qui néglige ce risque s'expose à des conséquences potentiellement désastreuses pour sa réputation, son fonctionnement, ses intérêts juridiques et ses finances.

Objectifs de l'examen et structure du rapport

Les principaux objectifs visés par le présent examen sont les suivants : a) relever et analyser les problèmes et les risques auxquels les entités des Nations Unies sont communément confrontées, à titre individuel, dans le cadre de leur cybersécurité, ainsi que les moyens par lesquels chacune y fait face, en gardant à l'esprit les exigences propres à chacune d'entre elles (perspective verticale) ; b) examiner les dynamiques interentités actuelles qui sont propices à une stratégie de cybersécurité à l'échelle du système, en vue d'améliorer la coordination, la collaboration et le partage de l'information parmi les entités des Nations Unies, et se pencher, le cas échéant, sur les possibilités de solutions mutualisées (perspective horizontale).

À partir des auto-évaluations fournies par les entités participantes, les Inspecteurs commencent par donner, dans le chapitre II, un aperçu du paysage de la cybersécurité tel qu'il se présente au système des Nations Unies, décrivant les types de menaces et de moyens d'attaque les plus courants, ainsi que leurs effets, tels qu'ils ont été rapportés, et attirent l'attention sur certaines questions techniques appelant plus ample examen. Dans le chapitre III, les Inspecteurs examinent les dispositions institutionnelles et les pratiques associées en vigueur dans les entités des Nations Unies, au regard d'une série de facteurs clés relevés dans le cadre de l'examen comme contribuant à la cyberrésilience institutionnelle ; le cas échéant, ils soulignent les bonnes pratiques. Dans le chapitre IV, l'accent est mis sur les structures interentités visant à encourager la coordination et la collaboration parmi les entités des Nations Unies ainsi que sur les capacités opérationnelles permettant la mise au

point et la mise en service de solutions partagées, là où elles ont un sens. Les spécialistes conviennent que le dispositif de chaque entité en la matière doit s'inscrire dans le prolongement de ses caractéristiques et exigences propres (selon son mandat, les informations qu'elle détient ou gère, son exposition aux risques, ses ressources, etc.). Cela étant, les entités des Nations Unies ne fonctionnent pas en vase clos et sont à bien des égards interconnectées, y compris par les programmes communs et une certaine interdépendance selon les mandats et les activités. Il est par conséquent crucial de délimiter les zones d'exposition communes et de rechercher celles qui se prêtent à une approche concertée.

La cybersécurité dans le système des Nations Unies

Il n'est pas une seule entité des Nations Unies qui puisse prétendre n'avoir subi aucune forme de cyberattaque, majeure ou mineure. Les actes malveillants visant l'utilisateur final du système informatique (hameçonnage ou *phishing*, usurpation d'identité, attaque « de l'homme du milieu », etc.) ou son infrastructure (logiciel malveillant, attaque par déni de service distribué, etc.) sont de loin les sources de menaces les plus souvent signalées. Bien que les menaces à la cybersécurité soient habituellement associées à des opérations techniquement sophistiquées, la communauté des spécialistes remarque un déplacement des attaques, traditionnellement dominées par le piratage des serveurs, réseaux et appareils finals, vers le piratage psychologique qui, à des fins illicites, notamment frauduleuses, amène les individus à divulguer des informations sensibles. La pandémie de maladie à coronavirus (COVID-19) a exacerbé les risques liés au piratage psychologique : plus des deux tiers des entités participantes ont signalé une forte augmentation des menaces et des vulnérabilités en matière de cybersécurité pendant les confinements mondiaux qui ont déconnecté de nombreux utilisateurs des ressources de cybersécurité centralisées.

En revanche, les effets des incidents qu'ont connus les entités participantes, tels qu'ils ont été rapportés, sont apparus limités. Ce fait pourrait amener à conclure prématurément qu'il n'y a pas lieu de s'inquiéter outre mesure. Ce n'est pas la conclusion à laquelle sont arrivés les Inspecteurs. Les données recueillies mettent nécessairement en évidence l'existence d'angles morts, notamment ceux résultant d'une réticence compréhensible à révéler le degré de vulnérabilité connu d'une entité et ceux tenant à la nature opaque des activités du cyberespace en général, ce qui donne à penser que l'étendue exacte des menaces et de leurs conséquences peut tout simplement ne pas être connue. Le plus souvent, surtout dans le cas d'attaques plus sophistiquées, les adversaires n'ont aucun intérêt à révéler leur présence ni les vulnérabilités dont ils ont tiré parti, d'où la probabilité que le nombre d'atteintes portées aux systèmes et de fuites de données subies soit sensiblement plus élevé que celui qui a été rapporté. Si la proportion des « inconnues connues » est grande par rapport à ce qui est connu de l'ampleur de la menace qui pèse sur la cybersécurité, la part des « inconnues inconnues » risque d'être plus préoccupante encore. C'est pourquoi il serait peu judicieux de juger de la gravité de la menace en se fondant sur la mesure dans laquelle elle s'est apparemment matérialisée par le passé. La probabilité de subir des dommages reste élevée ; elle appelle une attention soutenue et doit demeurer une préoccupation prioritaire.

Inégalité des degrés de maturité et de certains aspects de l'état de préparation technologique des entités

Le présent examen n'avait pas pour vocation de fournir une évaluation exhaustive de la robustesse des dispositifs opérationnels ou de l'infrastructure technique de chaque entité participante, mais de donner la mesure des capacités générales dont elles disposaient et de cerner certaines questions qui pourraient mériter une attention particulière. Pour des raisons évidentes associées au sujet du présent examen, les Inspecteurs ont choisi de ne pas révéler précisément les dispositions institutionnelles dont la divulgation pourrait compromettre la sécurité des entités concernées. Sans perdre de vue les limitations inhérentes aux informations recueillies principalement par auto-évaluation, de même que les variations considérables du degré de précision avec lequel les réponses lui ont été fournies, le Corps commun d'inspection (CCI) a constaté des différences marquantes entre les approches adoptées par les entités participantes pour faire face aux menaces pesant sur leur cybersécurité et, partant, entre les degrés de maturité de leurs dispositifs en la matière. Ces différences peuvent s'expliquer par les facteurs suivants : le contexte dans lequel chaque

entité fonctionne ; les exigences imposées par le type de données qu'elle détient ; la compréhension que son équipe dirigeante a de la cybersécurité et le degré de priorité qu'elle lui accorde ; sa propre perspective historique ; la disponibilité de ressources ; la grande variété des systèmes et outils informatiques ainsi que des solutions logicielles utilisées dans le système.

Les entités participantes estimaient avoir bien compris les aspects techniques centraux de la cybersécurité et leur avoir réservé des investissements correspondant à leurs capacités propres. Pour ce qui est des capacités technologiques et opérationnelles, les Inspecteurs ont limité leur analyse à la mise en exergue d'une série de questions qui mériteraient une plus ample attention, telles que : la gestion des appareils finals et les outils facilitant le travail à distance, en particulier dans le contexte de la pandémie de COVID-19 ; les risques associés au maintien de systèmes informatiques préexistants, acquis par le passé ou construits au sein de l'entité au fil du temps, qui pourraient ne plus être compatibles avec les logiciels et correctifs de sécurité modernes ; l'expansion continue de l'utilisation de l'informatique en *cloud* (ou en nuage) ; les dispositions institutionnelles de gestion des vulnérabilités ; le recours à l'informatique fantôme qui utilise et met en place des outils technologiques ne relevant pas du cadre informatique officiel de l'entité. Il est à noter que, malgré tous les problèmes qu'elle a causés, la pandémie a aussi été l'occasion d'évolutions positives. Les entités des Nations Unies ont ainsi été amenées à se pencher de plus près sur leurs cadres de gestion de la sécurité. Des projets institutionnels relatifs aux TIC ont commencé à se concrétiser pour répondre à des besoins immédiats. On peut dire que la migration massive et à brève échéance vers le travail à distance a conduit de nombreuses entités à renforcer d'urgence la sécurité de leurs accès à distance, et que cela peut avoir donné une impulsion bien nécessaire à la relance de l'action dans ce domaine.

Facteurs d'amélioration de la cyberrésilience

Les Inspecteurs se sont intéressés à une série de facteurs susceptibles d'améliorer le dispositif institutionnel de cybersécurité des entités des Nations Unies et leur capacité de cerner, de prévenir et de détecter les menaces à la cybersécurité, ainsi que de riposter aux incidents et de s'en remettre. Une approche à multiples facettes est requise, qui mobilise tous les niveaux de l'entité, y compris les organes délibérants et directeurs, les mécanismes de contrôle, la direction exécutive, les cadres moyens des unités administratives et organiques ou fonctionnelles, et le personnel dans son ensemble. La nature transversale des questions de cyberrésilience nécessite une perspective plus large qui dépasse les TIC, pour inscrire fermement la cybersécurité dans la gestion du risque institutionnel. Elle nécessite également une plus grande convergence entre la sécurité physique et la cybersécurité. Enfin, un dispositif de cybersécurité solide doit pouvoir compter sur des ressources humaines internes spécialisées, complétées par des services externes capables de répondre à des besoins spécifiques et ponctuels, ainsi que sur des ressources financières à la mesure des besoins de chaque entité. En somme, la mesure dans laquelle ces facteurs s'inscrivent dans la démarche de cybersécurité d'une entité influence directement sa cyberrésilience. Les Inspecteurs recommandent par conséquent que les chefs de secrétariat entreprennent une étude, à l'échelle de leur entité, de la mesure dans laquelle chacun des facteurs visés, tels qu'ils sont exposés plus loin, est intégré dans les politiques et pratiques de leur entité, et qu'ils rendent compte des résultats à leurs organes délibérants et directeurs pour recevoir des consignes sur les moyens de renforcer encore la cyberrésilience, compte tenu des forces et des faiblesses relevées dans ce processus (recommandations 1 et 2).

Orientations stratégiques et ressources à fournir par les organes délibérants et directeurs

Dans le système des Nations Unies, la cybersécurité continue d'être perçue comme une question essentiellement technique, ce qui peut expliquer pourquoi la mesure dans laquelle les organes délibérants et directeurs ont été appelés ou ont eux-mêmes demandé à s'investir dans la question, est restée modeste dans la plupart des entités à ce jour. Compte tenu des dimensions plus larges de la cybersécurité dont fait état le présent rapport, les Inspecteurs sont d'avis que les organes délibérants et directeurs devraient se mobiliser davantage en la matière, et fournir des orientations stratégiques de haut niveau en formulant

une déclaration explicite de l'appétit pour le risque de l'entité et en affectant les ressources nécessaires à la réalisation du niveau de protection souhaité. Plus généralement, la direction exécutive devrait réfléchir aux meilleurs moyens d'informer régulièrement les organes délibérants et directeurs des questions de cybersécurité, et d'utiliser ce processus pour faciliter les interactions avec ces organes, dans les limites de ce qui peut être considéré comme nécessaire et suffisant, sans compromettre les défenses de l'entité. Compte tenu de la nature abrupte des atteintes à la cybersécurité, et de l'impact significatif qu'elles peuvent avoir, les Inspecteurs conseillent également aux entités d'anticiper la nécessité de faire remonter aux organes délibérants et directeurs les informations concernant de telles atteintes, ainsi que la procédure à suivre pour ce faire, le cas échéant, à la fois sur le plan interne et parmi les membres des organes eux-mêmes.

Contribution de l'attention des organes de contrôle à l'amélioration des mesures de cybersécurité

Comme le confirme le présent examen, les mécanismes de contrôle internes et externes des entités des Nations Unies se sont intéressés aux questions de cybersécurité, même en l'absence de références explicites à cette matière dans leurs mandats. Les Inspecteurs ont pris connaissance de plusieurs exemples d'améliorations institutionnelles apportées au cadre de cybersécurité des entités participantes sur la base de recommandations de contrôle (par exemple, la création d'un poste de responsable de la sécurité de l'information, l'amélioration de la formation et l'adoption d'une feuille de route effectivement applicable). Les comités d'audit et de contrôle s'intéressent en fait à la cybersécurité dans le cadre de leur mandat relatif à la gestion du risque institutionnel, plutôt qu'en rapport avec la gouvernance des TIC. Il est louable que ces comités aient épousé le sujet, non seulement pour soutenir les équipes dirigeantes, mais aussi comme moyen d'informer les organes délibérants et directeurs des cyberrisques qui les concernent, leur permettant ainsi de contribuer à l'atténuation des risques au niveau de l'entité. Pour que la valeur ajoutée à la cybersécurité par tous les organes de contrôle soit maximale, il importe que les connaissances et l'expérience des spécialistes en la matière au sein de l'entité éclairent et alimentent le travail de la fonction de contrôle.

Cadres réglementaires, respect des règles et responsabilisation

Les entités participantes ont mentionné un large éventail de normes relatives à la cybersécurité, parfois plus d'une par entité. La plupart d'entre elles ont déjà obtenu la certification ISO 27001, envisagent de l'obtenir ou ont choisi de s'y conformer volontairement, sans chercher à officialiser la chose. Les Inspecteurs s'abstiennent de plaider en faveur de telle ou telle norme ou de l'adoption harmonisée, à l'échelle du système, de l'une ou l'autre d'entre elles, car différentes normes peuvent valablement servir différents objectifs et représenter des choix opportuns selon le degré de maturité des systèmes. Il semble cependant judicieux de s'inspirer − formellement ou informellement − des normes pertinentes pour la création et la gestion d'un cadre réglementaire propre. Il appartient donc aux entités participantes de sélectionner la norme qui leur convient et, dans le cadre de celle-ci, les mesures de référence les plus adéquates, compte tenu du degré de protection requis par leur situation et conformément aux exigences et aux risques relevés à l'issue d'une évaluation fiable et individualisée des cyberrisques.

Plusieurs grandes normes désignent l'existence de politiques et de procédures documentées en matière de cybersécurité comme une des composantes essentielles des mesures de contrôle qui sont à la base de la démarche d'une entité en matière de cybersécurité. Il s'avère qu'à quelques exceptions près, les entités participantes reconnaissent l'importance de disposer d'un cadre de référence clairement défini pour orienter la démarche de cybersécurité. À un niveau élevé, les stratégies relatives à l'informatique et aux communications comprennent généralement des considérations relatives à la cybersécurité, à des degrés de développement certes variables. Plus des deux tiers des entités ont mis en place des instruments de réglementation spécifiquement consacrés à la cybersécurité, et trois d'entre elles revoient actuellement leurs cadres, tandis que quatre s'emploient à mettre au point des politiques en la matière. Par ailleurs, pour quatre entités participantes, la fonction de cybersécurité et son cadre réglementaire peuvent être qualifiés tout au plus

d'embryonnaires. La question du respect des consignes en vigueur, s'agissant plus particulièrement des mesures coercitives en cas de non-respect de ces consignes, ne permet pas de conclure avec confiance à l'existence d'une culture institutionnelle de la cybersécurité dans l'ensemble du système. De l'avis des Inspecteurs cet aspect des choses mérite un examen plus attentif et appelle des approches plus nuancées pour renforcer la responsabilisation en cas de violation et, de façon plus générale, pour protéger les entités.

L'établissement d'une culture de la cybersécurité vient d'en haut

Le premier pas vers l'établissement d'une culture de la cybersécurité est franchi lorsque l'équipe de direction elle-même prend conscience des risques ainsi que des conséquences que peut avoir une hygiène informatique douteuse. Le personnel de direction doit se montrer plus actif et veiller à ce que soient mis en place des mécanismes internes de gouvernance qui lui fournissent les informations et les éléments de fait dont il a besoin. Le rôle de la direction exécutive ne se limite pas à décider de l'affectation des ressources. Un élément clé de ce rôle consiste à encourager une culture interne dans laquelle le fait de reconnaître et de répertorier en permanence la survenue d'incidents n'est pas vécu comme un échec, mais comme un point de départ pour résoudre un problème partagé et mieux protéger l'entité et ses actifs. Il est d'autres moyens concrets par lesquels la direction exécutive peut susciter l'action et influencer les mentalités en aval de la chaîne de commandement : en donnant l'exemple des comportements recommandés, en veillant à la responsabilisation des cadres dans toute l'entité, en prenant part à des programmes de sensibilisation et en faisant montre d'un style de direction investi dans les questions de cybersécurité. Une transformation culturelle doit se produire au sein du système des Nations Unies, et il est essentiel pour cela que les directions exécutives donnent le ton au sommet.

Intégration de la cybersécurité en tant que démarche à l'échelle de l'entité

La prise de conscience croissante du fait que la cybersécurité ne saurait être l'affaire des seuls services responsables des TIC a amené la majorité des entités participantes à reconnaître, d'une façon ou d'une autre, que les unités administratives comme organiques ont un rôle à jouer dans ce domaine. Il ressort toutefois des informations recueillies au cours du présent examen que des services de toutes catégories n'étaient pas encore assez ouverts à la nécessité d'inclure des critères de cybersécurité et de résilience dans la conception et l'exécution de leurs projets et activités. Dans certains cas, les règles et procédures de cybersécurité sont considérées comme un obstacle à la rapidité d'exécution plutôt que comme un bouclier servant à protéger la réputation et les actifs des entités. Il est particulièrement important que les chefs de secrétariat s'emploient à démentir de telles perceptions. Rendre plus explicite le rôle que la cybersécurité est appelée à jouer dans le cadre des fonctions organiques et administratives peut réduire les malentendus concernant les rôles et les responsabilités complémentaires de différents services et pallier le défaut d'appropriation détecté parmi certaines parties prenantes au cours du présent examen. Le fait d'intégrer des considérations de cybersécurité dans les règles et pratiques qui président aux activités de tous les services reviendrait à reconnaître que chaque fonction d'une entité doit contribuer à l'approche institutionnelle en la matière.

Le personnel comme première ligne de défense

La nécessité de sensibiliser chaque membre du personnel au rôle qu'il lui appartient de jouer dans la protection de l'information et des actifs numériques de son entité, ainsi qu'à l'importance d'observer les règles, les procédures et les meilleures pratiques en matière de cybersécurité, reste un défi de taille. Le facteur humain a gagné en importance non seulement dans le paysage des menaces à la cybersécurité, comme l'atteste la préoccupation générale suscitée par le fait que l'utilisateur final individuel est de plus en plus souvent pris pour cible, mais aussi comme élément important de la structure de défense des entités participantes, d'où la nécessité d'une information adéquate des individus concernés. La réalisation que la protection contre les menaces à la cybersécurité commence par l'utilisateur, bien informé et vigilant, a déclenché d'importants efforts de formation et de sensibilisation, malgré les ressources limitées, une certaine lassitude des utilisateurs face aux formations et la difficulté de rester informé de l'évolution constante du sujet. Il semble toutefois que les nombreux

programmes et initiatives à cet égard ne soient pas menés d'une façon qui soit cohérente, systématique ou axée sur la gestion des risques. Les Inspecteurs conseillent aux entités de s'attacher à mettre sur pied un programme de formation et de sensibilisation complet qui soit un outil dynamique de changement de la culture interne, moyennant des objectifs clairement définis pour chaque catégorie de parties prenantes, en fonction du risque qu'elle peut représenter pour l'entité, plutôt que de proposer des modules de formation séparés à tout un chacun, sans véritable projet stratégique. Il est également crucial de s'occuper des utilisateurs occasionnels des systèmes informatiques et de communication institutionnels, notamment les représentants participant aux conférences, les stagiaires, les visiteurs et d'autres catégories de non-fonctionnaires, dès lors que, souvent, ces personnes se connectent à l'infrastructure institutionnelle au moyen d'appareils personnels. Sans compter que comme elles ne font pas fréquemment usage des systèmes en question, elles risquent d'être moins au fait de l'usage correct et sûr qui doit en être fait, dans le respect des règles et des pratiques de l'entité.

Optimisation des dépenses et des investissements de cybersécurité

Il est difficile d'estimer les ressources actuellement consacrées à la cybersécurité. Cela est dû aux caractéristiques des cadres financiers et budgétaires des entités des Nations Unies, ainsi que des pratiques de gestion et de comptabilisation de ces ressources . Il va sans dire qu'un cadre de cybersécurité bien protégé a un coût. Malgré l'augmentation rapportée des ressources consacrées à la cybersécurité, les praticiens du système des Nations Unies perçoivent encore le manque de moyens comme un obstacle à la prise en charge par les entités de tous les aspects de leur cyberrésilience. Il est important de garder à l'esprit que le montant consacré à la cybersécurité n'est pas en corrélation automatique avec le niveau de protection. La clé n'est pas tant de savoir combien dépenser, mais de déterminer où affecter les ressources le plus utilement possible. Indépendamment des montants disponibles, il ressort des informations recueillies que les priorités de financement de la cybersécurité ne sont pas établies de façon cohérente par les entités des Nations Unies, ce qui accroît le risque d'inefficacité dans l'utilisation de ressources déjà rares. Pour optimiser les dépenses de cybersécurité, de même que les investissements associés, une analyse approfondie des cyberrisques, débouchant sur un dossier de décision précisant les coûts, avantages, risques et économies escomptées, et renvoyant également aux retombées financières possibles d'un renoncement à l'investissement envisagé, est une condition préalable à l'octroi par les organes délibérants et directeurs d'un niveau adéquat de ressources.

Capacités internes spécialisées en cybersécurité

Plus de la moitié des entités participantes se sont dotées de capacités internes en ressources humaines spécialisées et exclusives, allant d'un unique spécialiste de la sécurité de l'information, parfois même affecté à temps partiel, à une unité administrative plus étoffée sous la direction d'un responsable de la sécurité de l'information. Par contre, dans 10 entités participantes, les tâches relevant de la cybersécurité sont assurées principalement par des fonctionnaires chargés de la gestion des TIC, en même temps que leurs autres responsabilités. Le domaine de la cybersécurité fait fréquemment appel à des spécialistes externes en raison de sa nature techniquement complexe, en constante évolution, qui nécessite un degré de spécialisation considérable, et qu'il est difficile et coûteux de maintenir à disposition et à niveau de façon permanente. Le recours à des fournisseurs externes pour renforcer et compléter les capacités internes est chose inévitable et même souhaitable, en ce qu'il permet de répondre aux évolutions rapides du cyberespace. La mesure dans laquelle cette solution est utilisée est laissée à l'appréciation de chaque entité, compte tenu des besoins et du contexte qui lui sont propres. De l'avis des Inspecteurs, il importe toutefois que les entités maintiennent un niveau suffisant de contrôle, de supervision et de capacités techniques internes pour assurer les fonctions d'encadrement et d'interface vis-à-vis des capacités provenant de fournisseurs externes. Le fait de disposer d'un responsable de la sécurité de l'information à cet égard peut être porteur de l'attention et de l'assurance nécessaires. Les fonctions principales qui sont du ressort du responsable de la sécurité de l'information dépassent l'élaboration de mesures de contrôle au niveau opérationnel et incluent par défaut une dimension d'encadrement, de sorte que les considérations de cybersécurité puissent intervenir autant que possible dans la gestion des risques et de la résilience de l'entité.

Ayant constaté, entre les arrangements internes des entités participantes, des disparités qui pourraient être davantage à l'image de leurs limitations que de choix délibérés ou stratégiques, les Inspecteurs estiment que le fait de disposer, au sein d'une entité, d'un savoir-faire spécialisé en matière de cybersécurité contribue à renforcer le dispositif de l'entité elle-même, mais aussi du système tout entier, et qu'il s'agit par conséquent d'un investissement intéressant. Il serait en outre prudent pour chaque entité d'évaluer dans quelle mesure elle pourrait tirer avantage de l'établissement d'un centre des opérations de sécurité, même sous sa forme la plus rudimentaire, moyennant une analyse coûts-avantages spécifique assortie de paramètres tels que la complexité de l'infrastructure informatique et de communication, le nombre et le type des actifs et des processus critiques gérés, le volume global des flux de données et, partant, la fréquence des menaces. Un des aspects importants de l'officialisation d'un centre des opérations de sécurité, quelles que soient sa taille et sa capacité, est la place qu'il accorde à la surveillance quotidienne des opérations, aux fonctions cruciales de coordination et de synchronisation et à la sensibilisation institutionnelle, autant d'éléments qui peuvent être déterminants pour la bonne affectation des ressources et des capacités internes.

La cybersécurité : une priorité à l'échelle du système ?

Le renforcement du dispositif de cybersécurité du système des Nations Unies par l'intensification de la coordination et de la collaboration entre ses entités au niveau stratégique, et par le perfectionnement des capacités opérationnelles à l'échelle du système, sont des priorités affirmées de longue date, aussi bien par les États Membres que par les directions exécutives. Cependant, en dépit de la disponibilité de plusieurs ressources, mécanismes et initiatives d'importance au sein du système, et de l'existence apparente d'une volonté politique allant dans ce sens, les signes que ces déclarations ambitieuses donnent lieu à des progrès concrets sont loin d'être évidents. À ce stade, le système ne dispose pas d'une entité qui soit officiellement chargée de mener le programme d'harmonisation de la cybersécurité, les efforts déployés à l'échelle du système en matière de cybersécurité étant institutionnellement concentrés autour de mécanismes de coordination interentités relevant du Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination, avec un certain appui, sur le plan opérationnel, du Centre de calcul international des Nations Unies, qui fournit certains services partagés à plusieurs entités des Nations Unies. Dans le cadre du présent examen, les Inspecteurs ont constaté que les liens entre les orientations stratégiques et les capacités opérationnelles à l'échelle du système étaient insuffisants, et que ce fait avait affecté la dynamique entre ces deux structures et risquait de coûter cher en gains d'efficience non réalisés, les occasions de collaboration plus directe n'ayant pas été saisies.

Nécessité d'un niveau de protection de base et d'exigences de défense minima

L'idée selon laquelle une faible protection contre les menaces à la cybersécurité dans une entité rend tout le système plus vulnérable est généralement acceptée. Il est donc logique de dire que le système des Nations Unies est aussi fort que son maillon le plus faible. Toutefois, les initiatives lancées par le passé pour établir des repères communs ou des évaluations comparatives des niveaux de maturité en la matière n'ont pas bénéficié d'un soutien suffisant, leurs détracteurs invoquant la diversité des environnements structurels et contextuels dans lesquels les entités fonctionnaient comme un obstacle limitant la valeur de telles approches collectives ou cumulatives. À cela s'ajoute le peu d'enthousiasme de la part des équipes de direction des entités participantes pour la communication d'informations relatives à leur cybersécurité, considérées comme confidentielles ou comme susceptibles d'exposer des vulnérabilités, même au sein du cercle des entités elles-mêmes. Ces préoccupations pourraient être apaisées par la conclusion d'accords qui régiraient le partage de l'information et fourniraient les garanties nécessaires. Les tentatives d'instaurer des capacités opérationnelles au niveau du système, en matière de prévention, de détection et de riposte face aux menaces à la cybersécurité, n'ont pas encore donné de résultats tangibles. Certaines lacunes à cet égard ont été comblées par le Centre international de calcul des Nations Unies (CIC), dont le portefeuille de services de cybersécurité a attiré une large clientèle ; à cela près qu'en raison de leur caractère optionnel, ces prestations ne répondent

que partiellement aux besoins du système. Malgré les faibles résultats qu'ont donnés à ce jour les efforts déployés en faveur d'une approche commune ou concertée à l'échelle du système, que ce soit au niveau conceptuel ou au niveau opérationnel, les Inspecteurs estiment que la fixation d'un niveau minimum de protection et d'exigences minimales de défense pour les entités des Nations Unies, et donc pour le système dans son ensemble, reste un objectif valable, qui mérite d'être poursuivi.

Mécanisme interentités pour la cybersécurité

Il a été établi que la structure interentités consacrée à la cybersécurité existait de longue date et que, de façon générale, elle fonctionnait, même si certains des objectifs ambitieux qu'elle avait adoptés ne s'étaient pas encore traduits par des résultats tangibles, du moins au-delà des solides bases de partage d'informations et d'échanges professionnels qu'elle avait déjà permis à l'échelle du système. Les documents officiels du Réseau Technologie et numérique, rattaché au Comité de haut niveau sur la gestion, attestent que la cybersécurité figure à l'ordre du jour du système depuis 30 ans au moins. Depuis 2011, le Groupe d'intérêt pour la sécurité informatique, qui fonctionne sous la supervision du Réseau Technologie et numérique, est le principal mécanisme de promotion de la coopération et de la collaboration interentités visant à optimiser la sécurité de l'information au sein de ses organisations membres. Le partage de connaissances est le principal objet que lui confère son mandat, dont la modification de 2018 met aussi l'accent sur la réalisation de projets conjoints. Cette aspiration s'est trouvée encore amplifiée lorsque le Réseau a appelé le Groupe d'intérêt à jouer un rôle plus actif dans la conception et la diffusion de solutions et d'innovations partagées. Tout en reconnaissant la crédibilité professionnelle du Groupe d'intérêt et le corpus considérable de ses travaux réalisés au fil des ans, les Inspecteurs ont dû constater que le volet de son mandat relatif à l'élaboration de solutions partagées à l'intention du système n'avait pas été exécuté. En tant qu'organe de coordination, le Groupe d'intérêt rencontre les mêmes problèmes à cet égard que tout autre mécanisme interentités dénué du pouvoir de décision qui lui permettrait de forcer l'action directement au niveau du système. C'est pourquoi il ne serait pas réaliste d'espérer que des mesures concrètes soient prises dans ce cadre. L'influence du Groupe d'intérêt est limitée par le fait qu'il dépend de l'engagement et de la persévérance individuels des entités qu'il réunit, par les niveaux d'autonomie inégaux de ses membres au sein de leurs propres structures institutionnelles, et par le fait que lui-même est dépourvu des capacités opérationnelles qui lui permettraient de mettre en œuvre les accords conclus et les recommandations formulées. En outre, le Groupe d'intérêt est placé sous l'autorité du Réseau, ce qui reproduit la structure prédominante constatée dans la plupart des entités, à savoir que le responsable de la sécurité de l'information est placé sous l'autorité du responsable du service des TIC, avec tous les avantages et les inconvénients que cela suppose.

Le Centre international de calcul des Nations Unies en tant que fournisseur clé de services de cybersécurité au système

Le Centre international de calcul des Nations Unies fournit depuis plusieurs années des services de cybersécurité aux deux tiers environ des entités des Nations Unies, bien que la clientèle de chacun des 13 services concernés varie grandement. Cet aspect du catalogue de prestations du Centre s'est considérablement étoffé et diversifié, même si cette activité ne représente encore qu'une menue portion de son budget. Il a été constaté que ses services de cybersécurité avaient reçu des appréciations variables de la part des entités participantes et que son service de renseignements sur les menaces, *Common Secure Threat Intelligence*, était considéré comme son service phare. En 2019 déjà, le CCI avait appelé à une meilleure exploitation du potentiel non réalisé du Centre, en particulier dans le domaine de la cybersécurité. Les entités des Nations Unies et le Centre sont encouragés à élargir leurs domaines de coopération pour que les premières puissent compléter leurs capacités internes au moyen de services mutualisés supplémentaires. Dans cette optique, les chefs de secrétariat sont invités à revoir les arrangements actuels au niveau de leurs entités et à réexaminer les possibilités d'utiliser les services de cybersécurité du Centre. Le modèle d'activité du CIC, en tant qu'outil interentités soumis aux règles et au cadre administratif de l'Organisation mondiale de la Santé, combine les principes de récupération des coûts et de services partagés.

Cette combinaison s'est avérée à la fois favorable et contraire à la réalisation du projet du Centre de devenir une plaque tournante de la cybersécurité pour le système. Elle a créé une situation dans laquelle l'offre de services du Centre était tributaire du financement d'amorçage que des clients souhaitaient consacrer à la conception de tel ou tel nouveau service en réponse à la demande, alors que de nombreuses entités ne pourraient se permettre d'acquérir un service ainsi conçu que lorsqu'une masse critique de clients s'y seraient abonnés. Étant donné les défis que présente la cybersécurité et les risques auxquels sont confrontées les entités, il a été jugé opportun d'envisager le recours aux contributions volontaires en tant que mécanisme de financement complémentaire. Il permettrait de disposer de ressources plus directes aux fins de la préservation du dispositif global de cybersécurité du système. Les Inspecteurs considèrent que la création d'un fonds d'affectation spéciale destiné à compléter les mécanismes de financement existants au moyen de contributions volontaires, spécialement destinées à renforcer la cybersécurité du système au moyen de solutions partagées, a le potentiel de changer la donne face à certains des écueils rencontrés dans ce domaine. Outre qu'il permettrait aux États Membres qui le souhaitent de contribuer directement aux améliorations de la cybersécurité du système, le fonds serait aussi l'occasion, selon un mécanisme de gouvernance à concevoir par les parties prenantes compétentes, d'améliorer les liens entre les orientations stratégiques qui peuvent être fournies par le Groupe d'intérêt pour la sécurité informatique et les capacités opérationnelles mises à disposition par le Centre (recommandation 3). L'Assemblée générale est invitée à prendre acte de la recommandation et à solliciter des contributions au fonds d'affectation spéciale (recommandation 4).

Vers un meilleur alignement de la sécurité physique et de la cybersécurité

Il est bien connu que le Département de la sûreté et de la sécurité a pour mandat à l'échelle du système d'établir les politiques et de guider les dispositions opérationnelles relatives à la sûreté et à la sécurité physiques globales des entités. Malgré la convergence de l'espace physique et du cyberespace lorsqu'il s'agit de protéger le personnel et les actifs institutionnels, ce mandat, tel qu'il a été arrêté par l'Assemblée générale, porte sur des menaces spécifiques à la sûreté et à la sécurité physique telles qu'elles relèvent des attributions du Département, et ne contient par conséquent aucune référence à la cybersécurité ou aux risques et menaces qui la concernent. La nécessité d'un meilleur alignement entre la sécurité physique et la cybersécurité a certes été débattue dans le cadre de plusieurs organes interentités au fil des ans, mais ces discussions n'ont pas encore débouché sur des conclusions applicables au niveau du système. Pour préciser les possibilités et les risques que présenterait une extension au cyberespace de l'approche fondée sur la gestion des risques, d'une part, et sur la riposte structurée autour des responsabilités, d'autre part, qui caractérise le système de gestion de la sécurité des Nations Unies, les Inspecteurs recommandent que le Secrétaire général présente à l'Assemblée générale un rapport qui expose les moyens d'assurer une protection plus globale du personnel et des actifs des Nations Unies et qui indique, en conséquence, les mesures qui seraient nécessaires pour renforcer les structures existantes, en accordant une attention particulière au rôle que pourrait jouer le Département de la sûreté et de la sécurité à cet égard. Le rapport devrait être éclairé par les résultats de consultations à mener entre les mécanismes interentités de coordination saisis de la cybersécurité et le Réseau interorganisations de gestion des mesures de sécurité, moyennant la contribution du CIC, selon les besoins (recommandation 5).

Recommandations

Recommandation 1

Les chefs de secrétariat des entités des Nations Unies devraient établir, à titre prioritaire et d'ici à la fin de 2022, un rapport exhaustif sur leur cadre de cybersécurité, qui aborde les facteurs d'amélioration de la cyberrésilience examinés dans le présent rapport, et présenter ce document, dans les meilleurs délais, à leurs organes délibérants et directeurs.

Recommandation 2

Les organes délibérants et directeurs des entités des Nations Unies devraient examiner les rapports des chefs de secrétariat sur les facteurs d'amélioration de la cyberrésilience et fournir des orientations stratégiques concernant les améliorations à mettre en œuvre, le cas échéant, dans leurs entités.

Recommandation 3

Le Directeur du Centre international de calcul des Nations Unies devrait s'employer à établir, d'ici à la fin de 2022, un fonds d'affectation spéciale pour recevoir les contributions de donateurs destinées à renforcer les capacités du Centre en matière de conception, de mise au point et de prestation de services et de solutions partagés pour développer le dispositif de cybersécurité des entités des Nations Unies.

Recommandation 4

L'Assemblée générale des Nations Unies devrait, au plus tard à sa soixante-dix-septième session, prendre acte de la recommandation adressée au Directeur du Centre international de calcul des Nations Unies d'établir un fonds d'affectation spéciale pour les solutions de cybersécurité partagées et inviter les États Membres qui souhaitent renforcer le dispositif de cybersécurité des entités des Nations Unies à contribuer au fonds.

Recommandation 5

Le Secrétaire général devrait présenter à l'Assemblée générale des Nations Unies, au plus tard à sa soixante-dix-huitième séance, un rapport ayant pour objet d'étudier de nouvelles possibilités de mettre à profit la convergence entre la sécurité physique et la cybersécurité pour assurer une protection plus globale et intégrée du personnel et des actifs des Nations Unies, et d'indiquer les mesures qui seraient nécessaires pour renforcer les structures existantes en conséquence, en accordant une attention particulière au rôle que pourrait jouer le Département de la sûreté et de la sécurité à cet égard.

Ces recommandations formelles sont complétées par 35 recommandations informelles ou « souples », libellées en caractères gras dans le corps du rapport ; ce sont des suggestions supplémentaires dont la mise en œuvre pourrait, de l'avis des Inspecteurs, renforcer le dispositif de cybersécurité du système des Nations Unies.

Table des matières

		Page
	Résumé analytique	iii
	Abréviations	xv
I.	Introduction	1
	A. Contexte	1
	B. Objectifs, portée et méthodologie	3
	C. Définitions	6
II.	Bref état des lieux de la cybersécurité dans le système des Nations Unies	9
	A. Attention croissante accordée à la cybersécurité et inégalité des degrés de maturité	9
	B. Paysage des menaces à la cybersécurité	10
	C. Effets connus et inconnus des atteintes à la cybersécurité	13
	D. Dialogue et coopération avec les autorités nationales	15
	E. État de préparation technologique et questions appelant examen	16
III.	Facteurs d'amélioration de la cyberrésilience	22
	A. Mobilisation des organes délibérants et directeurs	22
	B. Incorporation de la cybersécurité dans la gestion du risque institutionnel	25
	C. Parti à tirer de la convergence entre sécurité physique et cybersécurité	27
	D. Élaboration de cadres réglementaires pour le respect des règles et la responsabilisation	29
	E. Mise à profit des contributions des mécanismes de contrôle	34
	F. Établissement d'une culture de la cybersécurité : du sommet à la base	36
	G. Adoption d'une démarche à l'échelle de l'entité	38
	H. Importance du personnel en tant que première ligne de défense	39
	I. Affectation optimale de ressources financières à la cybersécurité	43
	J. Investissement dans des ressources humaines spécialisées	47
	K. Réflexion et communication sur les efforts d'amélioration de la cyberrésilience déployés à l'échelle de l'entité	52
IV.	La cybersécurité à l'échelle du système	54
	A. La cybersécurité : une priorité pour l'ensemble du système ?	54
	B. Les mécanismes interentités ayant trait à la cybersécurité	57
	C. Les services de cybersécurité du Centre international de calcul des Nations Unies	62
	D. Le renforcement des liens systémiques entre orientation stratégique et capacités opérationnelles	68
	E. Les possibilités d'harmoniser davantage sécurité physique et cybersécurité	72
Annexes		
I.	Les axes de travail intergouvernementaux relatifs à la cybersécurité et à la cybercriminalité	76
II.	Quelques aspects de la cybersécurité abordée sous l'angle de la gestion des risques	79
III.	Les principales normes relatives à la cybersécurité utilisées par les entités participantes du Corps commun d'inspection	83

IV. Les cadres réglementaires des entités des Nations Unies en matière de cybersécurité 83

V. Les structures administratives chargées de la cybersécurité et leurs rattachements hiérarchiques au sein des entités participantes du Corps commun d'inspection (janvier 2021) 87

VI. Les dispositions interentités d'ordre institutionnel et opérationnel concernant la cybersécurité... 89

VII. Récapitulatif des services du Centre international de calcul des Nations Unies utilisés par des entités participantes du Corps commun d'inspection (janvier 2021) 90

VIII. Tableau comparatif de l'état des adhésions aux entités chargées de questions de cybersécurité (janvier 2021) 92

IX. Glossaire de termes relatifs à la cybersécurité..... 94

X. Vue d'ensemble des mesures que les entités participantes sont appelées à prendre conformément aux recommandations du Corps commun d'inspection..... 96

Abréviations

AIEA	Agence internationale de l'énergie atomique
BIT	Bureau international du Travail
CCI	Corps commun d'inspection
CCS	Conseil des chefs de secrétariat pour la coordination
CIC	Centre international de calcul des Nations Unies
CNUCED	Conférence des Nations Unies sur le commerce et le développement
FAO	Organisation des Nations Unies pour l'alimentation et l'agriculture
FNUAP	Fonds des Nations Unies pour la population
HCR	Haut-Commissariat des Nations Unies pour les réfugiés
ISO	Organisation internationale de normalisation
ITC	Centre du commerce international
OACI	Organisation de l'aviation civile internationale
OMI	Organisation maritime internationale
OMM	Organisation météorologique mondiale
OMPI	Organisation mondiale de la propriété intellectuelle
OMS	Organisation mondiale de la Santé
OMT	Organisation mondiale du tourisme
ONG	organisation non gouvernementale
ONUDC	Office des Nations Unies contre la drogue et le crime
ONUDI	Organisation des Nations Unies pour le développement industriel
ONU-Femmes	Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes
ONU-Habitat	Programme des Nations Unies pour les établissements humains
ONUSIDA	Programme commun des Nations Unies sur le VIH/sida
ONUV	Office des Nations Unies à Vienne
PAM	Programme alimentaire mondial
PNUD	Programme des Nations Unies pour le développement
PNUE	Programme des Nations Unies pour l'environnement
TIC	technologies de l'information et des communications
UIT	Union internationale des télécommunications
UNESCO	Organisation des Nations Unies pour l'éducation, la science et la culture
UNICEF	Fonds des Nations Unies pour l'enfance
UNOPS	Bureau des Nations Unies pour les services d'appui aux projets
UNRWA	Office de secours et de travaux des Nations Unies pour les réfugiés de Palestine dans le Proche-Orient
UPU	Union postale universelle

I. Introduction

A. Contexte

1. **L'importance de la cybersécurité à l'ère numérique.** Dans ce monde numérisé, la question de la cybersécurité a pris toute son importance pour les organisations internationales. Les entités des Nations Unies n'échappent pas à cette réalité. La transformation numérique, la dépendance croissante à l'égard des technologies de l'information et des communications (TIC) et des solutions en ligne, et le fait que les menaces à la cybersécurité ne cessent de se faire plus pressantes, tant par leur sophistication que par leur pouvoir de perturbation, ont donné lieu à une augmentation inédite des cyberrisques auxquels sont confrontées les entités des Nations Unies. Des incidents qui auraient été qualifiés d'extraordinaires par le passé deviennent aujourd'hui monnaie courante. Les Inspecteurs rappellent la lettre adressée au Secrétaire général, en 2017, par les représentants des organes de contrôle des entités des Nations Unies, à l'occasion de leur toute première réunion conjointe, dans laquelle ils faisaient figurer parmi les trois grands enjeux du système des Nations Unies la nécessité pour ses organes directeurs de prendre la juste mesure de l'existence de risques nouveaux et naissants, en particulier les menaces à la cybersécurité, avec leur envergure mondiale et leur capacité de compromettre les fonctions vitales du système, ainsi que les risques qui vont de pair avec les nouvelles façons de travailler nées d'une transformation numérique en plein essor[1]. C'est sur cette toile de fond que les entités participantes du Corps commun d'inspection (CCI) ont souscrit à l'examen des politiques et pratiques de cybersécurité en vigueur au sein du système des Nations Unies. Réalisé par le CCI au titre de son programme de travail pour 2020, cet examen est le dernier en date d'une série consacrée à des questions à caractère technologique, comme la gouvernance des TIC, la gestion des sites Web et l'utilisation des services d'informatique en *cloud* (ou en nuage)[2].

2. **Le système des Nations Unies cible de cyberattaques.** Le paysage des menaces qui pèsent sur la cybersécurité des Nations Unies ne diffère pas de celui auquel font face d'autres organisations, en ce que les instigateurs, les moyens et les objectifs, allant du financier au symbolique, sont les mêmes. S'il est une distinction, elle tient aux raisons pour lesquelles les entités des Nations Unies pourraient être considérées comme une cible plus intéressante que d'autres, privées ou publiques. Leur attrait pourrait tenir à leur visibilité particulière et à leur présence mondiale, qui leur confère, aux yeux du pirate informatique en quête de notoriété, un potentiel publicitaire plus évident que toute attaque contre une cible gouvernementale ou publique nationale. En outre, contrairement à de nombreuses cibles du secteur privé, elles peuvent présenter un intérêt particulier pour les hackers activistes ou « hacktivistes » qui, par idéologie, rejettent ou combattent les valeurs que représentent ou diffusent les entités des Nations Unies. À cela s'ajoute que la sphère intergouvernementale dans laquelle ces entités fonctionnent donne à leur situation une dimension politique indéniable, à laquelle elles-mêmes font à peine allusion, mais qui est un fait reconnu, sans exception. En bref, bien que les méthodes soient identiques, les motifs peuvent varier. Ce qui est clair, c'est que les cinq dernières années ont vu une augmentation exponentielle du nombre d'attaques de grande comme de petite envergure dirigées contre des entités participantes du CCI, comme il ressort des chiffres de diverses sources dont les Inspecteurs ont pris connaissance.

3. **Les atteintes à la cybersécurité susceptibles de compromettre l'exécution des mandats au-delà de la perturbation des systèmes.** La faiblesse du dispositif de cybersécurité d'une entité des Nations Unies peut avoir des répercussions qui vont au-delà de la perturbation des fonctions administratives et des systèmes et infrastructures informatiques et de communication et qui ne devraient pas se mesurer seulement au volume d'informations et de données compromises. Une seule défaillance peut avoir des effets dévastateurs pour l'entité si elle concerne des catégories de données sensibles telles que les informations qui permettent d'identifier des personnes, les dossiers médicaux des membres

[1] Lettre adressée au Secrétaire général, 26 janvier 2017.

[2] JIU/REP/2008/5, JIU/REP/2008/6, JIU/REP/2011/9 et JIU/REP/2019/5.

du personnel, les données tombant sous le coup de la propriété intellectuelle, les archives historiques et politiques ou autres documents de cet ordre. C'est aussi la capacité de l'entité d'exécuter son mandat et sa crédibilité aux yeux de ses États membres et de ses bénéficiaires qui sont en jeu. Dans la sphère où elle exerce ses activités, un incident même mineur sur le plan technologique peut occasionner des ondes de choc susceptibles de perturber des processus diplomatiques et intergouvernementaux, des interventions humanitaires, voire, dans le pire des cas, la paix et la sécurité internationales. S'il est vrai que les cyberattaques peuvent toucher différemment des entités des Nations Unies aux mandats et structures différents, la menace n'en reste pas moins réelle et partagée[3]. Certes, aucune entité ne sera jamais tout à fait à l'abri d'un incident de cybersécurité, quel que soit son niveau de préparation et de vigilance, mais celle qui néglige ce risque s'expose à des conséquences potentiellement désastreuses pour sa réputation, son fonctionnement, ses intérêts juridiques et ses finances.

4. **L'importance accordée à la cybersécurité par la communauté internationale et les Nations Unies.** Des rapports et des résolutions émanant d'organes délibérants et directeurs compétents ainsi que de mécanismes internes de coordination montrent que les activités hostiles du cyberespace sont perçues depuis le début des années 1990 au moins comme une menace pour la communauté internationale en général et les entités des Nations Unies plus particulièrement. Le sujet a fait l'objet d'un débat de fond mené parallèlement selon deux perspectives : d'une part, celle des gouvernements en tant que membres des organes délibérants et directeurs des Nations Unies préparant la riposte mondiale à l'émergence de la cybercriminalité et des menaces (c'est la dimension « extérieure » du travail que les Nations Unies consacrent à la cybersécurité et dont la coordination à l'échelle du système revient au Comité de haut niveau sur les programmes du Conseil des chefs de secrétariat pour la coordination (CCS)), et d'autre part, celle des entités des Nations Unies qui cherchent à renforcer leur état de préparation et leurs moyens de riposte internes face aux problèmes connexes, à la fois collectivement et individuellement (c'est la dimension « intérieure » qui relève du Comité de haut niveau sur la gestion). La reconnaissance de ce double rôle du système des Nations Unies ressort d'une déclaration finale faite par le Secrétaire général dans le cadre du CCS aussi récemment qu'en 2019, affirmant que le système « devait jouer un rôle de chef de file et définir une position unifiée en ce qui concernait la cybersécurité et les menaces connexes, tout en servant de plateforme de rassemblement pour les États membres et les autres parties prenantes afin de discuter de la cybersécurité sous toutes ses formes »[4].

5. **La responsabilité qui incombe aux États de protéger les actifs de l'ONU dans le cyberespace.** Pour ce qui est des protections juridiques dont elles jouissent en matière de cybersécurité, les entités des Nations Unies s'en remettent aux privilèges et immunités applicables à leurs biens, avoirs, archives, documents et communications au sens large[5]. L'existence de tels privilèges et immunités oblige les États parties à se donner les moyens, en vertu de leurs législations respectives, d'assurer aux entités concernées la protection et la sécurité qui leur sont nécessaires pour atteindre leurs buts, et en particulier l'inviolabilité de leurs locaux, archives et documents « quels que soient leur siège et leur détenteur ». Autrement dit, les États, notamment les pays hôtes, ont le devoir de protéger les entités des attaques dirigées contre elles, que ce soit dans la sphère physique ou numérique. Cette interprétation des textes pertinents a été confirmée aux Inspecteurs par le Bureau des affaires juridiques et règle la question de savoir si les données électroniques et les actifs numériques sont couverts par les dispositions juridiques en vigueur. En fait, le Bureau des affaires juridiques a indiqué que, plus récemment, le terme « archives » tel qu'il figurait dans le cadre d'accords de siège et d'autres accords avec des pays hôtes passés bilatéralement entre des entités et les pays qui les accueillaient sur leur territoire avait été expressément défini comme comprenant les messages électroniques et les fichiers informatiques, de même que tous

[3] Pour des informations générales sur les problèmes auxquels sont confrontées les entités des Nations Unies, voir la brochure « *UN Digital Blue Helmets* » que le Bureau de l'informatique et des communications a consacrée aux Casques bleus du numérique.

[4] CEB/2019/2, par. 39.

[5] Art. 105 de la Charte des Nations Unies ; Convention du 13 février 1946 sur les privilèges et immunités des Nations Unies ; Convention du 21 novembre 1947 sur les privilèges et immunités des institution spécialisées ; Accord du 17 août 1959 sur les privilèges et immunités de l'Agence internationale de l'énergie atomique.

documents similaires appartenant à l'entité concernée, ou détenue par celle-ci, dans l'exercice de ses fonctions. De façon similaire, les communications protégées ont été considérées comme comprenant la communication de données électroniques, tandis que d'autres accords ont été conçus de façon plus exhaustive, assurant l'inviolabilité de tout moyen de communication employé. Au sens le plus large, cela signifie que les États ont la responsabilité au regard du droit international de protéger les actifs des Nations Unies, y compris dans le cyberespace.

6. **La transition du domaine des TIC vers une conception plus large.** Les considérations de cybersécurité sont apparues et ont traditionnellement été prises en charge dans la sphère des TIC, domaine qui, aux premiers temps de l'informatique, occupait une place moins importante qu'aujourd'hui dans les activités des organisations. Cette conception de la cybersécurité en tant que discipline centrée sur les TIC était le produit logique d'une époque où les menaces étaient surtout limitées à l'infrastructure informatique et touchaient une gamme d'actifs informationnels et de modalités de fonctionnement bien plus restreinte. Cependant, à présent que ces technologies sont profondément implantées dans les activités des entités, et que le paysage des menaces s'étend bien au-delà des simples perturbations techniques aux solutions relativement simples et aux parades à caractère technologique, il ne semble plus viable de considérer la cybersécurité seulement sous l'angle restrictif des TIC. **En fait, les Inspecteurs sont d'avis que la cybersécurité devrait se concevoir sous un angle beaucoup plus large, englobant plusieurs domaines et compétences organisationnels, dont la gestion du risque institutionnel, la sécurité physique, la protection des données et de la vie privée, les connaissances juridiques et la sécurité de l'information dans le contexte plus large de la gestion de l'information et des connaissances.**

7. **La planification de la continuité des opérations au cœur d'une stratégie de cybersécurité fondée sur les risques.** Certaines organisations ont d'ores et déjà entrepris de faire figurer la cybersécurité parmi les nombreux aspects de leur gestion de la résilience. La préoccupation première à cet égard est d'évaluer correctement les cyberrisques avec comme double objectif d'adopter des mesures préventives d'atténuation des risques et de défense contre les menaces, d'une part, et de définir des protocoles régissant les dispositions à prendre et de préserver la continuité des opérations au cas où de tels risques et menaces se concrétiseraient, d'autre part. En matière de cybersécurité, l'atténuation des risques n'est jamais absolue, mais plutôt une question de degré, et son efficacité ne doit pas être jaugée à sa seule capacité de contrer les menaces, mais aussi à la mesure dans laquelle elle est capable de contribuer au rétablissement des opérations à la suite d'une attaque réussie. Il importe donc de disposer, en cas d'incident grave, d'une procédure éprouvée de reprise après sinistre pour tous les systèmes d'information utilisés. Tel ne peut être le cas que si les protocoles de reprise sont testés régulièrement et rigoureusement dans le cadre de la planification de la continuité des opérations, idéalement au moyen du puissant outil de gestion des risques qu'est le test d'intrusion. Bien qu'ayant une solide dimension technique, les procédures de reprise après sinistre devraient être conçues selon les paramètres stratégiques fixés par la direction de l'entité (comme la tolérance au risque, l'appétit pour le risque, les ressources disponibles) afin d'être efficaces. Il s'ensuit que la planification de la continuité des opérations devient, en même temps que la gestion des risques, un pilier indispensable de la résilience de l'entité face aux menaces physiques comme aux menaces à la cybersécurité[6].

B. Objectifs, portée et méthodologie

Objectifs

8. Les principaux objectifs visés par le présent examen sont les suivants :

a) Relever et analyser les problèmes et les risques auxquels les entités des Nations Unies sont communément confrontées dans le cadre de leur cybersécurité, ainsi que les moyens par lesquels chacune y fait face, en gardant à l'esprit leurs exigences communes ou propres, en fonction de leurs contextes respectifs, et leur capacité de protéger leurs principaux actifs tout en restant en mesure d'exécuter leurs mandats ;

[6] Le programme de travail du CCI pour 2021 prévoit l'examen de la continuité des opérations dans les entités des Nations Unies.

b) Répertorier les dispositions interorganisations actuelles et déterminer si elles sont propices à une stratégie de cybersécurité à l'échelle du système, et relever les possibilités d'améliorer, le cas échéant, la coordination, la collaboration et le partage de l'information parmi les entités des Nations Unies.

Portée

9. **Examen portant sur tout le système.** Le présent examen, entrepris à l'échelle du système, porte sur toutes les entités participantes du CCI, à savoir le Secrétariat de l'Organisation des Nations Unies et ses entités, les fonds et programmes des Nations Unies, d'autres entités des Nations Unies, les institutions spécialisées des Nations Unies et l'Agence internationale de l'énergie atomique (AIEA). Le Centre du commerce international (ITC) n'a pas pris part à l'examen et n'est donc pas inclus dans les chiffres globaux fournis dans le présent rapport. Le CCI a par ailleurs examiné le Centre international de calcul des Nations Unies (CIC) en tant que fournisseur de services de cybersécurité à plusieurs entités des Nations Unies.

10. **Examen portant sur les dispositions internes de cybersécurité.** Le présent rapport porte sur les dispositions prises dans le cadre de la gestion des cadres de cybersécurité au sein des entités des Nations Unies et qui visent à protéger leurs actifs dans le cyberespace et à assurer l'exécution des activités relevant de leurs mandats (la dimension « intérieure » de la cybersécurité)[7]. Le travail intergouvernemental accompli par le système des Nations Unies pour soutenir les États Membres, notamment par la fourniture d'une assistance technique destinée à renforcer les capacités nationales de cybersécurité ou à combattre la cybercriminalité, est résumé dans l'annexe I, à titre de contexte, dès lors qu'il ne relève pas de l'objet principal du présent examen. L'annexe contient un bref historique de l'évolution de la question selon les axes de travail de l'Assemblée générale et d'autres organes intergouvernementaux.

11. **Aspects techniques n'ayant pas été étudiés dans le détail.** Bien que la question de la cybersécurité ne soit pas purement technologique, elle ne saurait être abordée sans référence aux TIC. Les Inspecteurs n'ont toutefois pas entrepris d'analyse poussée de la pertinence et de la rationalité techniques des mesures prises par les entités. Lorsque l'examen de certains aspects techniques s'est avéré indispensable pour assurer la complétude du présent rapport, les Inspecteurs ont pu tirer parti de compétences spécialisées externes et se contenter de relever certains points appelant éventuellement un examen plus approfondi. On retiendra en particulier que l'objectif du présent rapport n'est pas de présenter une étude exhaustive, comparative ou autre, de la maturité de chaque entité des Nations Unies. Une telle évaluation a été considérée comme dépassant son cadre, mais aussi comme étant d'une utilité limitée pour les entités concernées, fût-ce collectivement ou individuellement.

12. **Domaines connexes centrés sur les données, concernés par la cybersécurité, mais débordant le cadre de l'étude.** Une variété de domaines relatifs à la gestion de l'information et des connaissances, à la protection des données et de la confidentialité et à d'autres sujets apparentés recoupent la question de la cybersécurité tout en débordant le cadre de la présente étude. Certains ont déjà fait l'objet de rapports du CCI (telle la classification de l'information dans le cadre de la gestion des dossiers et des archives)[8], d'autres sont en cours de normalisation au niveau de certaines entités en conformité avec les directives applicables à l'échelle du système (telle la transposition en politiques propres et en textes administratifs des principes en matière de protection des données personnelles et de la vie privée adoptés par le CCS en 2018). Par ailleurs, les défis et complexités tenant à l'introduction, la même année, du règlement général sur la protection des données de l'Union européenne et aux tentatives de lui donner vigueur au sein des entités des Nations Unies donnent lieu à une série distincte de questions qui ont pour la cybersécurité des implications débordant le cadre de la présente étude. Loin d'être exhaustive, cette liste de questions donne un aperçu de la vaste

[7] Le présent rapport est complété par une lettre d'observation adressée aux chefs de secrétariat des entités participantes du CCI, concernant les risques associés à la sauvegarde et à la protection des documents et des données juridiques, normatifs, administratifs, politiques et historiques des entités (JIU/ML/2021/1, en anglais).

[8] JIU/REP/2013/2.

portée de la cybersécurité en tant que matière transversale qui ne pouvait être abordée que sommairement dans le présent rapport. **Les Inspecteurs souhaitent appeler l'attention sur le fait que la protection des données et la confidentialité des informations personnelles en particulier sont des questions importantes par leur actualité et les préoccupations qu'elles suscitent, et qu'il serait opportun et justifié de consacrer un rapport critique aux pratiques et politiques des entités des Nations Unies en la matière.**

Méthodologie

13. Conformément aux normes et procédures de travail internes du CCI, les Inspecteurs ont utilisé plusieurs méthodes de collecte des données qualitatives et quantitatives provenant de différentes sources afin d'assurer la cohérence, la validité et la fiabilité de leurs conclusions. Les informations qui ont servi à l'établissement du présent rapport étaient à jour en mai 2021.

- **Questionnaires et étude documentaire.** Le CCI a recueilli des informations au moyen de deux questionnaires adressés à ses entités participantes. Les Inspecteurs ont examiné les dispositions pertinentes des cadres réglementaires applicables (résolutions des organes directeurs, stratégies internes en matière de TIC, politiques spécifiques et procédures à suivre concernant la sécurité de l'information et la cybersécurité, lorsqu'elles existaient) et compulsé des rapports établis par des organes de contrôle internes et externes. Une suite de demandes d'information adressées au CIC ont permis d'examiner son mandat, son catalogue de services et ses capacités institutionnelles et opérationnelles dans le domaine de cybersécurité. Le Bureau des affaires juridiques a fourni par écrit des éclaircissements sur une série de points juridiques. L'analyse des rapports des comités et réseaux du CCS, principalement le Réseau technologie et numérique et son Groupe d'intérêt pour la sécurité informatique, ont permis de mieux comprendre la dynamique interentités et les initiatives actuelles et passées à l'échelle du système. Les Inspecteurs ont également consulté les normes du secteur concernées et la littérature relative à la cybersécurité à titre de documentation générale.
- **Entretiens.** Se fondant sur les réponses aux questionnaires, les Inspecteurs ont mené 45 entretiens auprès de responsables des TIC, chargés de la cybersécurité en particulier, ainsi qu'auprès de hauts fonctionnaires pour s'informer de la façon dont la question se présentait à un niveau institutionnel plus large. Des entretiens ont été menés par la suite avec des représentants d'organes de contrôles, du Département de la sûreté et de la sécurité et de certaines entités non participantes. Les Inspecteurs se sont également entretenus avec le Président du Groupe d'intérêt pour la sécurité informatique et avec des représentants du secrétariat du CCS, ce qui leur a fourni des indications supplémentaires sur les initiatives de cybersécurité interentités. Les entretiens qu'ils ont eus avec des représentants du CIC leur ont permis d'obtenir des détails sur les capacités du Centre en matière de cybersécurité. Ils ont également assisté à l'édition 2020 de la conférence Common Secure organisée par le CIC et tenue virtuellement en raison de la pandémie de maladie à coronavirus (COVID-19), pour se faire une idée des évolutions et des difficultés qui intéressent les abonnés à ce service du CIC. Ils ont également bénéficié des points de vue et données d'expérience de plusieurs responsables de la sécurité de l'information, membres d'un réseau mondial informel de municipalités aux situations similaires, se mettant ainsi au fait des politiques et pratiques adoptées et des leçons retenues par ces autorités en tant qu'éléments pouvant servir de références issues du secteur public pour les entités des Nations Unies.

14. **Limites tenant à la disponibilité et à la confidentialité de l'information.** Des limites se sont imposées aux Inspecteurs, tenant principalement aux facteurs suivants : a) la disponibilité de l'information (étant donné que les paramètres des atteintes à la cybersécurité n'avaient pas été enregistrés de façon systématique ou l'avaient été sans suivre une méthode commune, ce qui limitait aussi la comparabilité des données) ; b) la confidentialité des données relatives aux menaces, incidents et ripostes, les entités estimant que la communication de ces informations leur faisait courir le risque inutile de voir localiser et révéler les vulnérabilités de leurs infrastructures de sécurité, ce qui explique que les

informations sont essentiellement présentées sous forme globale dans l'exposé du rapport, sans être associées à telle ou telle entité, sauf justification dans des cas particuliers ; c) les effets de la pandémie de COVID-19 sur la collecte des données, à savoir des retards et la nécessité de mener les entretiens par visioconférence, ce qui peut avoir affecté la disponibilité de certains interlocuteurs ainsi que leur disposition à communiquer par cette voie des informations sensibles qui auraient autrement pu être transmises dans le cadre de relations interpersonnelles. En outre, bien que les Inspecteurs aient souhaité étudier et rapporter comment les réactions des entités participantes à la pandémie avaient éclairé leurs considérations de cybersécurité, certaines dispositions prises à cet égard peuvent avoir évolué et ne pas avoir été pleinement prises en compte pendant le processus d'examen.

15. **Remerciements.** Les Inspecteurs souhaitent exprimer leur gratitude à tous les responsables des entités des Nations Unies et à tous les représentants d'autres organisations qui ont contribué à l'établissement du présent rapport, en particulier celles et ceux qui ont pris part aux entretiens et qui ont si volontiers partagé leurs connaissances et leur savoir spécialisés. À des fins de contrôle de la qualité, une méthode d'examen par les pairs a été utilisée pour recueillir les avis des Inspecteurs du CCI sur le projet de rapport, lequel a ensuite été transmis aux entités concernées de sorte qu'elles puissent livrer leurs commentaires de fond sur ses constatations, conclusions et recommandations, et en corriger les éventuelles erreurs de fait.

16. **Recommandations.** Le présent rapport contient cinq recommandations formelles, dont une s'adresse à l'Assemblée générale, une aux organes délibérants et directeurs, une aux chefs de secrétariat des entités participantes du CCI, une au Secrétaire général et une au Directeur du CIC. Pour faciliter l'utilisation du présent rapport, l'application de ses recommandations et le suivi de cette application, l'annexe X contient un tableau indiquant si le rapport a été soumis aux entités concernées pour suite à donner ou pour information, et précisant dans le premier cas si ce sont les organes délibérants et directeurs ou les chefs de secrétariat qui sont concernés. Les recommandations formelles s'accompagnent de 35 recommandations informelles, présentées en caractères gras. Ce sont des suggestions supplémentaires dont l'application, de l'avis des Inspecteurs, pourrait renforcer la cybersécurité du système des Nations Unies.

C. Définitions

17. **Absence de définition universellement reconnue de la cybersécurité.** Si les normes internationales et nationales régissant la sécurité de l'information comprennent souvent une définition de la cybersécurité, il n'existe pas de définition universellement reconnue du terme ni de consensus mondial sur ce qu'il recouvre précisément. Les Inspecteurs ont constaté de même qu'il n'y avait pas, dans le cadre des Nations Unies, d'orientation à l'échelle du système, émanant d'une instance compétente recommandant telle ou telle définition comme s'imposant à toutes les entités[9], non plus que les cadres réglementaires propres aux entités prises individuellement n'ont entrepris d'imposer une telle définition. Aux fins du présent rapport, les Inspecteurs retiennent la définition de la cybersécurité formulée par l'Union internationale des télécommunications (UIT), telle qu'elle est reproduite dans l'encadré 1. La grande majorité des entités participantes du CCI ont confirmé que cette définition correspondait à leur conception de la question, que venait fréquemment compléter la référence aux normes informatiques pertinentes.

[9] Le cadre sur la cybersécurité et la cybercriminalité à l'échelle du système des Nations Unies (voir CEB/2013/2) et le plan de coordination interne du système des Nations Unies sur la cybersécurité et la cybercriminalité (2014, annexe) comprenaient des définitions visant à assurer une compréhension commune des notions de cybercriminalité et cybersécurité, à ceci près qu'il s'agissait de définitions de travail, à vocation fonctionnelle, qui n'avaient pas été approuvées à proprement parler par le système des Nations Unies .

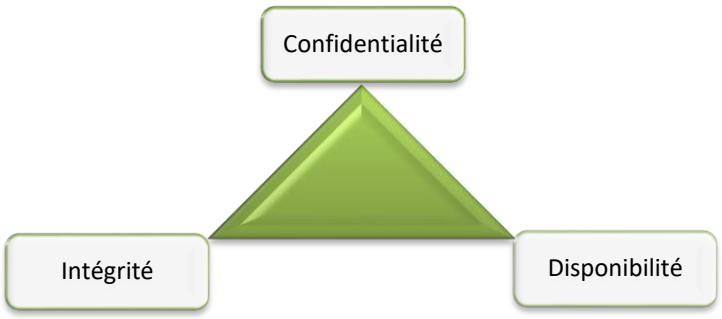
Encadré 1
La cybersécurité selon la définition de l'UIT

« **cybersécurité** : ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants : • Disponibilité • Intégrité, qui peut englober l'authenticité et la non-répudiation • Confidentialité. »

IUT, Recommandation ITU-T X.1205, *Présentation générale de la cybersécurité*.

18. **Sécurité de l'information et cybersécurité.** Les entités sont nombreuses à utiliser l'expression « sécurité de l'information » (*information security*), qui concerne l'information sous toutes ses formes, où qu'elle se trouve, sans se limiter aux données électroniques qui peuplent la sphère numérique. La cybersécurité (*cybersecurity*) se concevra plus volontiers en rapport avec une information purement numérique et la protection d'une gamme plus large d'actifs liés au cyberespace ou affectés par celui-ci, comme il ressort de la définition de l'UIT. Cette légère divergence conceptuelle des deux notions n'empêche pas qu'existe entre elles une vaste intersection où elles ont notamment en commun la protection des trois objectifs centraux que sont la confidentialité, l'intégrité et la disponibilité de l'information (c'est la « triade de la sécurité de l'information » représentée à la figure I, souvent appelée « triade confidentialité, intégrité et disponibilité »). Pour certaines entités, « cybersécurité » et « sécurité de l'information » sont des notions tout à fait interchangeables ; pour d'autres, « cybersécurité » a remplacé la notion plus traditionnelle de « sécurité de l'information », même si cela revient à omettre les préoccupations plus larges relatives à la gestion des connaissances et de l'information en faveur d'une approche plus centrée sur les TIC ; d'autres encore voient dans le terme « cybersécurité » une notion qui englobe à la fois celle de « sécurité de l'information » et celle, plus étroite (et plus rarement utilisée), de « sécurité des TIC », qui s'entend spécifiquement de la sécurité de l'infrastructure informatique et de communication (par exemple, les matériels, les logiciels, les réseaux et les processus techniques).

Figure I
Modèle de la triade de la sécurité de l'information[10]



Source : National Institute of Standards and Technology (États-Unis d'Amérique).

[10] Telle que définie par le Center for Internet Security, la triade confidentialité-intégrité-disponibilité est un modèle de référence conçu pour orienter et évaluer la façon dont une organisation gère les données qu'elle stocke, transmet ou traite. Chaque élément de la triade constitue une composante cruciale de la sécurité de l'information. La « confidentialité » renvoie au fait que les données ne devraient pas être

19. Des ambiguïtés terminologiques comparables ont été constatées dans la nomenclature des fonctions dirigeantes sous lesquelles la cybersécurité tendait à être placée au sein d'une entité. Ainsi, le responsable « de la sécurité de l'information » peut-il travailler sous les ordres d'un responsable « de l'informatique et des communications », « de l'informatique » ou « de l'information ». À ce niveau supérieur, soit les titres sont synonymes et se rapportent à la direction du département des TIC, soit le responsable de l'information dirige également la gestion des connaissances et des dossiers ou la communication et les relations publiques. Il n'a pas été possible de discerner de schéma cohérent qui aurait donné à conclure que la différenciation des responsabilités se rattachant à chaque titre résultait d'une volonté ou d'une rigueur conceptuelles.

20. Les Inspecteurs utilisent dans tout le rapport le terme « cybersécurité » tel qu'il est défini ci-dessus. Toute référence à la « sécurité de l'information » ou à la « sécurité informatique » est faite délibérément, dans le souci de respecter les sources citées ou l'usage correct de termes techniques tels que « responsable de la sécurité de l'information » ou « système de gestion de la sécurité de l'information ». Les Inspecteurs ont estimé qu'il n'était pas nécessaire de revoir cette nomenclature ni de l'harmoniser, dès lors qu'elle n'entravait pas la communication ou l'échange d'informations connexes parmi les entités.

accessibles ou lisibles sans autorisation. Il s'agit d'en réserver l'accès aux parties autorisées. Les attaques contre la confidentialité sont fondées sur la divulgation. L'« intégrité » renvoie au fait que les données ne devraient en aucune manière être modifiées ou compromises. Il s'agit de les maintenir dans l'état voulu et d'en réserver la modification aux parties autorisées. Les attaques contre l'intégrité sont fondées sur la modification. La « disponibilité » renvoie au fait que les données devraient être accessibles sur demande légitime. Il s'agit de veiller à ce que les parties autorisées puissent y accéder librement lorsqu'elles en ont besoin. Les attaques contre la disponibilité sont fondées sur la destruction.

II. Bref état des lieux de la cybersécurité dans le système des Nations Unies

A. Attention croissante accordée à la cybersécurité et inégalité des degrés de maturité

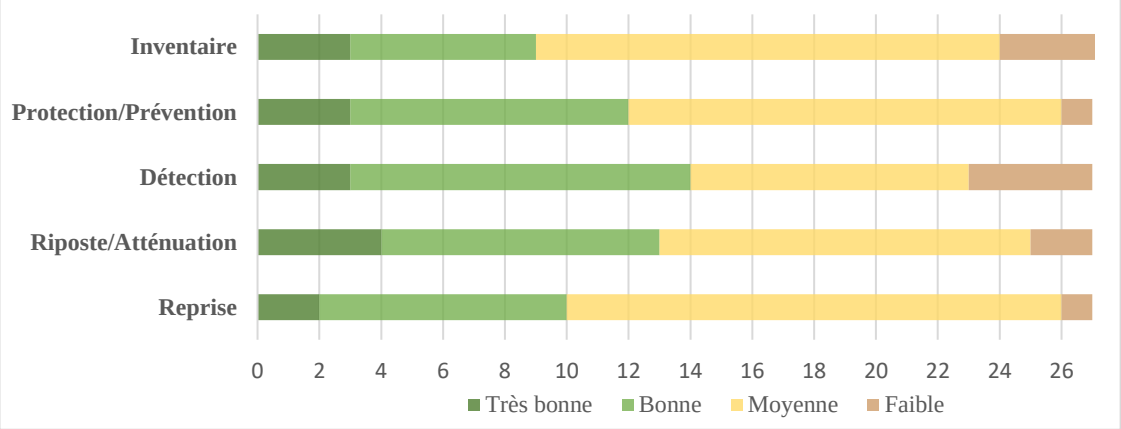
21. **Une prise de conscience croissante de la place à accorder à la cybersécurité.** Il y a eu, ces dernières années, parmi les entités des Nations Unies, une prise de conscience croissante, quoique inégale, de l'importance à accorder à la cybersécurité. L'exposition et l'attrait des entités des Nations Unies comme cibles de cyberattaques est incontestable, bien que ce risque puisse varier selon le mandat et la visibilité de l'entité concernée. On peut dire que le mandat ou le modèle de fonctionnement, de même que l'information détenue ou gérée, sont des facteurs qui ont influé sur la cadence à laquelle les entités ont pris acte de l'importance à reconnaître à la cybersécurité. Celles qui ont à traiter des données politiquement sensibles, susceptibles d'avoir une incidence sur la sécurité internationale ou des intérêts économiques nationaux, et celles qui ont à brasser de grands volumes de données juridiquement sensibles, notamment des données personnelles relatives à des populations bénéficiaires souvent vulnérables, semblent avoir entrepris avant d'autres la mise à jour de leurs dispositifs de cybersécurité, tandis que d'autres, aux mandats relativement peu controversés, se sont engagées sur la voie de la cyberdéfense avec moins d'empressement. À cela viennent s'ajouter les entités qui se sont trouvées sous les feux de l'actualité en raison de leur mandat et ont dû à brève échéance redoubler d'efforts en la matière (comme l'Organisation mondiale de la Santé (OMS)), et celles pour lesquelles des cyberattaques de grande envergure ou de grande visibilité ont précipité la nécessité d'agir et de renforcer promptement la cyberrésilience (comme l'Organisation de l'aviation civile internationale (OACI)). Dans l'ensemble, cependant, toutes les entités participantes du CCI ont pris conscience, sous une forme ou une autre, de l'importance de disposer d'une cybersécurité robuste, à la hauteur de leurs exigences opérationnelles.

22. **L'inégalité des degrés de maturité des entités des Nations Unies.** Bien qu'aucune entité participante du CCI ne soit apparue comme ayant ignoré la nécessité d'investir dans sa cybersécurité, des différences sensibles ont été constatées dans la façon dont les unes et les autres avaient répondu aux menaces à leur cybersécurité. Des variations significatives du degré de maturité de leurs cadres de cybersécurité ont été constatées, même en l'absence de points de référence communs ou de critères uniformément appliqués qui auraient permis de les comparer selon une méthode fiable et sur la base de données factuelles. Ces différences peuvent s'expliquer par les facteurs suivants : le contexte dans lequel chaque entité fonctionne ; les exigences imposées par le type de données qu'elle détient ; la mesure dans laquelle sa direction comprend la cybersécurité et le degré de priorité qu'elle lui accorde ; la disponibilité de ressources ; la disparité des systèmes et outils informatiques ainsi que des solutions logicielles utilisées, résultant souvent d'années de décisions d'investissement et de choix de fournisseurs non coordonnés dans l'ensemble du système. S'il existe indubitablement des caractéristiques communes, structurelles et autres, entre la plupart, voir la totalité, des entités examinées par le CCI, le projet de fournir une évaluation définitive du degré de maturité global atteint par le système des Nations Unies dans son ensemble en matière de cybersécurité n'aurait pas rendu compte de la diversité qui caractérise ses membres. Un tel exercice est en outre apparu d'une valeur pratique limitée, dès lors que la comparaison avec d'autres membres ou la détermination d'une maturité « moyenne » à l'échelle du système n'auraient guère éclairé les entités sur leur propre protection.

23. **Il y a matière à amélioration selon les réponses recueillies.** L'état des lieux approximatif que tente de dresser la figure II montre comment les entités elles-mêmes ont évalué leur cadre global de cybersécurité selon les grands domaines définis dans le questionnaire du CCI. L'interprétation des réponses reçues, en l'absence de cadre de référence commun ou de points de comparaison, n'est certes pas sans difficultés, mais le profil général qui se dessine, même dans ce cadre subjectif, n'est pas celui d'une cybersécurité bien affirmée à l'échelle du système. Dans la mesure où il pouvait fournir des indications concernant sa clientèle, le CIC, ayant posé les mêmes questions dans sa propre

évaluation de la performance des entités des Nations Unies, a donné à celles-ci des appréciations qui allaient de « moyen » à « faible », ce qui vient confirmer qu'il y a matière à amélioration au niveau du système.

Figure II
Auto-évaluation de la performance des entités participantes du CCI dans les grands domaines de la cybersécurité, par type de contrôles et nombre d'entités



Source : Questionnaire du CCI (2020).

Note : Les catégories soumises à l'auto-évaluation sont inspirées de celles qui sont utilisées dans les cadres de référence et les normes reconnus dans le domaine de la cybersécurité. Aux fins du questionnaire du CCI, la cybersécurité s'entend des domaines suivants : l'inventaire (fonctions critiques, actifs, ressources, risques, etc.) ; la protection et la prévention (gestion de l'accès, sensibilisation, formation, procédures, technologie, etc.) ; la détection (anomalies et incidents, surveillance continue, processus de détection, etc.) ; la riposte et l'atténuation (planification, communications, analyse, atténuation, etc.) ; la reprise (planification, rétablissement, communications, améliorations, etc.).

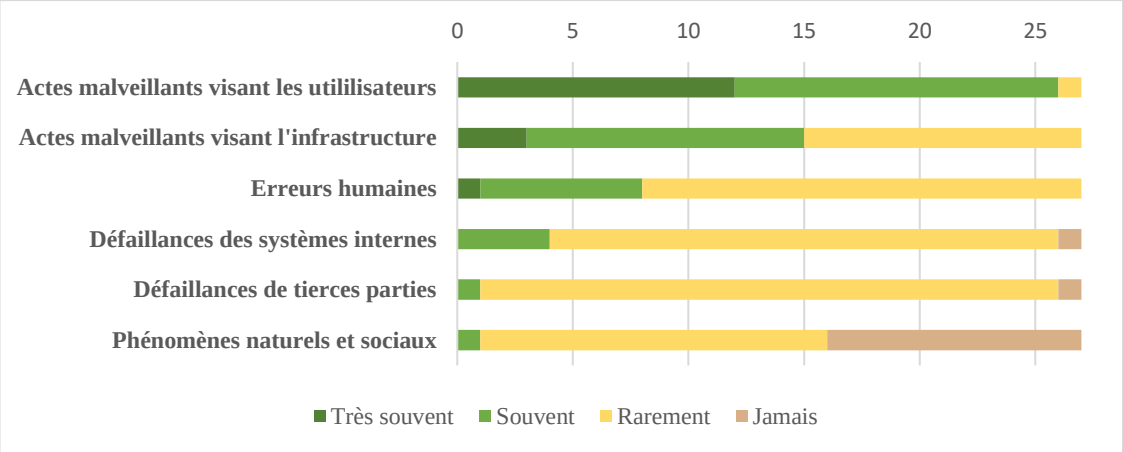
24. **Les risques augmentent à l'échelle du système par suite de la faiblesse des dispositifs individuels.** La question de l'état de préparation requis en matière de cybersécurité ne se résume pas aux risques qui pèsent sur chaque entité individuellement. Au cours des entretiens, des spécialistes de la cybersécurité ont souscrit au constat qu'une entité vulnérable, dont les défenses accusaient des faiblesses, représentait un risque pour les autres entités du système. De fait, une fois que l'attaquant a acquis les droits administratifs qui lui permettent de pénétrer plus profondément dans les systèmes informatiques de l'une d'entre elles, il peut exploiter cette brèche pour pénétrer le territoire numérique d'une autre. Le déplacement latéral malveillant d'une entité à une autre (le fait pour l'attaquant de « pivoter ») peut aussi être difficile à détecter et à contrer, car il peut se confondre avec le trafic normal. En se servant des informations recueillies au sein de l'infrastructure d'une entité, le hacker peut affiner encore sa méthode d'attaque et mettre une série de techniques et outils mieux adaptés au service de son objectif. Il s'ensuit que les entités qui qualifient de « faible » leur performance en matière de cybersécurité constituent un problème collectif. Il est donc permis de dire que le système des Nations Unies est aussi fort que son maillon le plus faible. Cette caractéristique est explorée plus avant dans le chapitre IV du présent rapport.

B. Paysage des menaces à la cybersécurité

25. **Les principales sources de menace et les moyens d'attaque les plus courants.** L'aperçu que la figure III donne de l'exposition actuelle aux menaces, est basé sur les réponses fournies par les entités participantes du CCI concernant la fréquence des incidents, considérés selon la source des menaces, qui les avaient affectés au cours des cinq dernières années. Les actes malveillants visant l'utilisateur final du système informatique (hameçonnage ou *phishing*, usurpation d'identité, attaque « de l'homme du milieu », etc.) ou l'infrastructure informatique elle-même (logiciel malveillant, attaque par déni de service distribué, etc.) étaient de loin les types de menaces le plus souvent signalés. Les responsables interrogés ont confirmé que, dans un passé récent, les actes malveillants visant les utilisateurs

finals avaient été les attaques les plus courantes et celles qui avaient connu la plus grande progression. La pandémie a aggravé la situation, de nombreux utilisateurs finals ayant été forcés de travailler à distance, souvent avec des moyens privés, occasionnant une pression supplémentaire, dans de nombreux cas et à divers degrés, sur les moyens de protection de la cybersécurité institutionnelle (par. 39 à 41).

Figure III
Menaces à la cybersécurité enregistrées par les entités participantes du CCI au cours des cinq dernières années, par source de menace et nombre d'entités



Source : Questionnaire du CCI (2020).

Note : Les sources des menaces ont été précisées comme suit : actes malveillants visant les utilisateurs (hameçonnage ou *phishing*, vol d'identité, attaque « de l'homme du milieu », etc.) ; actes malveillants visant l'infrastructure (logiciel malveillant, attaque par déni de service distribué, autres actes d'ordre technique, etc.) ; erreurs humaines (erreur de configuration, erreur opérationnelle, non-respect des procédures, perte de matériel, etc.) ; défaillances des systèmes internes (dysfonctionnement d'un appareil ou d'un système, panne du matériel, panne de courant, panne d'une ligne de communication, etc.) ; défaillances de tierces parties (fournisseurs de services Internet, réseau électrique, gestion des appareils à distance, etc.) ; phénomènes naturels et sociaux (inondation, tremblement de terre, explosifs, troubles, incendie, etc.).

26. **La progression des attaques de piratage psychologique, en particulier pendant la pandémie de COVID-19.** Bien que les menaces à la cybersécurité soient habituellement associées à des opérations techniquement sophistiquées dirigées contre des infrastructures, la communauté de la cybersécurité des Nations Unies a signalé un déplacement des attaques, traditionnellement dominées par le piratage des serveurs, réseaux et appareils finals, vers le piratage psychologique qui, à des fins frauduleuses, amène les individus à divulguer des informations sensibles. La pandémie de COVID-19 a exacerbé les risques liés au piratage psychologique. Plus des deux tiers des entités participantes ont signalé une forte augmentation des menaces et des vulnérabilités en matière de cybersécurité pendant les confinements mondiaux qui ont effectivement déconnecté de nombreux utilisateurs des ressources de cybersécurité centralisées. Le passage soudain au travail à distance rend moins direct le contact de l'utilisateur avec un professionnel formé qui pourrait le conseiller face à un courriel ou un site Web suspects. Selon le CIC, les cybercriminels et les adversaires ont profité de la confusion créée par la pandémie et de l'intérêt accru suscité par les contenus relatifs à cette actualité pour diffuser des messages d'hameçonnage consacrés à la COVID-19 et créer de faux sites Web chargés de logiciels malveillants prétendant fournir des informations sur la maladie. Les attaques par hameçonnage ou *phishing* se sont avérées particulièrement efficaces pendant cette période, qui a également été marquée par la diffusion d'un volume sans précédent de désinformation, parfois à des fins d'exploitation.

27. **La problématique particulière du piratage psychologique.** Contrairement aux attaques dirigées contre l'infrastructure, qui visent directement un nombre limité de ressources informatiques dont la protection peut s'avérer plus aisée, le piratage psychologique est considéré comme problématique à plusieurs égards. Techniquement simple à appliquer, il est conçu pour toucher simultanément un grand nombre d'utilisateurs et maximiser ainsi les chances de violation. En outre, bien que ces procédés visent les

utilisateurs finals, ils ne servent souvent que de point d'entrée vers d'autres actifs critiques. De telles intrusions, facilitées par des membres du personnel à leur insu, peuvent passer inaperçues pendant des années, ce qui facilitera encore l'accès des adversaires à l'architecture de sécurité et aux informations confidentielles du système, qui leur ouvriront, à leur tour, de nouvelles possibilités d'attaque. Parmi celles-ci, le pivot, technique utilisée pour se déplacer latéralement de l'environnement informatique d'une entité à celui d'une autre, à la suite de la pénétration initiale, en tirant parti des éléments d'infrastructure partagés ou liés. C'est une tactique particulièrement préoccupante pour les entités des Nations Unies, dont bon nombre partagent locaux, centres de données et serveurs, car elle rend les entités les plus avancées et les mieux protégées aussi vulnérables que les maillons les plus faibles de chaîne. Il est donc particulièrement important de veiller à ce que tous les effectifs d'utilisateurs soient bien formés et sensibilisés en vue de renforcer les pratiques salutaires.

28. **Les autres menaces.** Les entités ont également mentionné les erreurs comme source non négligeable de vulnérabilités : erreurs de configuration, erreurs opérationnelles, non-respect des procédures, perte de matériel ou dégâts accidentels causés par un manque de conscience plus général de ces questions. Les défaillances de tiers seraient plus rares, ce qui est encourageant quant au soin avec lequel les entités sélectionnent leurs partenaires commerciaux. Les catastrophes naturelles et autres dangers, dont les perturbations causées par les conflits ou les activités terroristes, auraient été les menaces les moins courantes, selon les réponses. Elles n'en constituent pas moins un domaine important où les considérations de sécurité physique et de cybersécurité doivent aller de pair pour atténuer les retombées.

29. **Les origines des menaces.** Dans le contexte des Nations Unies, et de façon plus générale d'ailleurs, les atteintes à la cybersécurité peuvent être le fait d'une grande variété d'auteurs de menace (encadré 2), appartenant à l'entité ou étrangers à celle-ci, qui peuvent agir à dessein (attaque délibérée) ou involontairement (par des actions ou des omissions accidentelles ou en étant instrumentalisés à leur insu). Certains groupes criminels proposent leurs capacités en louage à d'autres acteurs, lesquels sous-traitent ainsi effectivement leurs attaques en recourant à la « cybercriminalité en tant que service ». D'où la difficulté de répondre à la question de savoir qui est à l'origine d'une attaque donnée (attribution de la menace), ne serait-ce qu'en raison de la myriade de mécanismes qui existent pour dissimuler l'origine effective des attaques (comme la mystification ou *spoofing*, la gestion de réseaux de zombies ou *bot herding*, etc.). De fait, plusieurs responsables interrogés ont reconnu que les entités des Nations Unies ne manquaient pas seulement de moyens pour déterminer de façon fiable les origines des attaques, mais qu'elles hésitaient aussi à en entreprendre l'attribution, car les dépenses à engager pour ce faire dépasseraient de loin les avantages ou l'utilité de connaître les responsables des intrusions. Ils ont été nombreux à indiquer qu'ils préféraient consacrer leurs efforts à la prévention, la détection et la riposte, plutôt qu'investir du temps et des ressources dans la recherche des adversaires, ce qui demanderait des efforts considérables et ne résoudrait pas le problème car, quand bien même il serait mis fin aux attaques concernées, les entités continueraient d'en subir de nouvelles. Il en était de même des menaces persistantes avancées qui, de l'aveu des entités, étaient un phénomène non négligeable tendant à prendre la forme d'intrusions, de surveillances et d'effets à retardement qui supposaient un niveau de ressources et de perfectionnement généralement associé aux attaques parrainées par des États.

Encadré 2
Principaux types d'auteurs de menace dans le cyberenvironnement

- **Hackers ou pirates informatiques**. Individus ou groupes qui s'introduisent dans les réseaux pour causer des perturbations, des dommages ou le chaos, principalement à la recherche de notoriété ou de sensations fortes.
- **Hacktivistes**. Hackers animés d'une motivation particulière qui conçoivent leurs actes comme une forme de désobéissance civile ou comme un moyen d'expression politique ou idéologique.
- **Cybercriminels**. Acteurs qui se livrent à des activités criminelles facilitées par le cyberespace (infractions courantes, telles que la fraude, le vol et l'extorsion, commises par des moyens informatiques) ou dépendantes de lui (propagation de virus ou de logiciels malveillants et autres activités qui ne peuvent être menées que par des moyens informatisés). Compte tenu de leur niveau de perfectionnement technique et de leur capacité d'organisation, les acteurs en question peuvent aller de la petite opération à de vastes réseaux de criminalité organisée.
- **Espions industriels**. Acteurs, parfois considérés comme une sous-catégorie du groupe criminel, qui se spécialisent dans l'obtention de secrets d'affaires, le chantage pour des motifs d'intérêt économique ou le sabotage contre la concurrence, et qui opèrent principalement dans le monde des affaires.
- **États ou groupes parrainés par des États**. Acteurs hautement perfectionnés, dotés de ressources importantes, dont les activités tendent à être difficilement détectables, traçables et identifiables, et qui peuvent poursuivre furtivement des objectifs complexes, souvent indirects et peu évidents, en étant directement employés ou indirectement financés par des organes gouvernementaux ou militaires. Par le passé, les États disposaient surtout de capacités d'investigation, mais c'est un fait généralement admis que ces dernières années, certains se sont aussi dotés de capacités offensives.
- **Acteurs internes**. Acteurs qui, en raison d'une relation contractuelle avec l'entité concernée, ne sont pas considérés comme externes, mais mettent l'entité en danger de l'intérieur. Il peut s'agir entre autres d'employés mécontents ou de personnel employé ou contractuel insuffisamment formé.

C. Effets connus et inconnus des atteintes à la cybersécurité

30. **Les effets sont qualifiés de limités.** Pour mieux comprendre la mesure dans laquelle les risques ont donné lieu à des atteintes à la cybersécurité affectant les entités participantes, le CCI a demandé à celles-ci de classer les incidents qu'elles avaient connus selon leur gravité (d'insignifiant à grave) et selon les domaines sur lesquels ils avaient eu des répercussions (financier, opérationnel, numérique, politique ou relatif à la réputation, matériel ou physique, ou relatif à la productivité). Il est intéressant, et peut-être surprenant, que dans leurs réponses, les entités participantes aient invariablement qualifié de mineures ou d'insignifiantes les retombées des incidents de cybersécurité auxquels elles avaient été confrontées, quel qu'ait été le type de ces retombées. Il est parallèlement reconnu que le nombre et la fréquence des atteintes à la cybersécurité évitées est énorme, de l'ordre de plusieurs milliers de cas par mois, et que ces faits ont connu une croissance exponentielle ces dernières années. Ce constat est révélateur du volume de menaces à la cybersécurité qui pèsent sur les entités et leur infrastructure aujourd'hui. Il reste que, de prime abord et sans perdre de vue le fait que la collecte systématique de données à ce sujet est pratiquement inexistante, les répercussions demeurent, dans l'ensemble, limitées.

31. **Les domaines les plus affectés.** Les entités ont indiqué que les domaines les plus affectés par les cyberattaques (les effets ont été qualifiés de « modérés » par un nombre comparativement plus élevé, quoique toujours limité, d'entités, alors qu'une ou deux les ont qualifiés d'« importants », mais aucune de « graves ») avaient été le numérique (fuites de données principalement), suivi par les dommages politiques et à la réputation (fausses informations, représentation défavorable dans les médias, interférence indue dans les

processus intergouvernementaux, etc.). Même sur le plan financier, les pertes directes (transferts de fonds frauduleux notamment) n'avaient représenté que de modestes montants, ce qui pourrait donner à conclure, non sans prudence, que les mesures de contrôle s'étaient avérées efficaces à cet égard. Les Inspecteurs souhaitent toutefois relever d'autres conséquences financières des cyberattaques (telles que les heures de travail et les frais nécessaires pour établir les faits et déterminer l'étendue des dommages, les frais de récupération des actifs et des équipements, le coût afférent aux services de conseil externes requis pour résoudre les failles, les pertes de productivité dues aux pannes ou aux périodes d'indisponibilité des systèmes, ou le coût des investissements consacrés à la prévention de futurs problèmes) qui peuvent être beaucoup plus difficiles à quantifier, mais qui sont indubitablement appréciables. Globalement, malgré le fait que la majorité des entités participantes aient qualifié leur capacité de riposte de « moyenne » (un tiers seulement l'ayant jugée « forte » ou « très forte »), les effets des incidents de cybersécurité constatés dans le système des Nations Unies de nos jours, tels qu'ils ont été rapportés, ne semblent pas particulièrement préoccupants.

32. **Une réalité inconnue.** Plusieurs facteurs donnent toutefois à penser que la cybersécurité doit faire l'objet d'une attention prioritaire. Premièrement, les données recueillies mettent en évidence l'existence d'angles morts qui confirment que l'étendue exacte des menaces et de leurs conséquences est inconnue, comme plusieurs entités l'ont reconnu dans leurs réponses. Le plus souvent, surtout dans le cas des attaques plus sophistiquées, les adversaires n'ont aucun intérêt à révéler leur présence ni les vulnérabilités dont ils ont tiré parti, d'où la probabilité que les atteintes portées aux systèmes et les fuites de données aient atteint des niveaux sensiblement plus élevés que ceux dont il a été rendu compte. À cet égard, plusieurs interlocuteurs ont signalé que la proportion des « inconnues connues », par rapport à ce qui était connu de l'ampleur des menaces qui pesaient sur la cybersécurité, était grande, mais que la part des « inconnues inconnues » risquait d'être plus préoccupante encore. Deuxièmement, il est possible que dans leurs réponses, les interlocuteurs aient (volontairement ou involontairement) minimisé les effets des incidents, car dans une culture institutionnelle régie par l'information sur la performance et caractérisée par un fort sentiment de dépendance vis-à-vis des ressources liées à ces informations, la franche reconnaissance des faiblesses n'est pas encore devenue la règle. Les constatations peuvent s'en trouver faussée. À titre d'exemple, dans leur réponse au questionnaire du CCI, 11 entités ont officiellement déclaré avoir récemment subi au moins une cyberattaque importante qui avait eu des effets sur leurs opérations. Cependant, certaines entités dont il est de notoriété publique qu'elles ont fait l'objet de telles attaques n'ont pas révélé ces faits dans leurs échanges avec le CCI. Il est donc permis de supposer que les menaces effectives ainsi que leurs effets dépassent à la fois ce qui est connu et ce que les entités sont disposées à signaler.

33. **La distinction entre menaces passées et incidents à venir.** Indépendamment de ce qui précède, les experts semblent s'accorder sur le fait qu'il serait peu judicieux de juger de la gravité des menaces existantes en se fondant sur la mesure dans laquelle elles se sont apparemment matérialisées par le passé. La probabilité de subir des dommages reste élevée et devrait être anticipée par la mise en place précoce de contre-stratégies. Par exemple, la menace croissante que représente le déploiement de logiciels rançonneurs aux fins d'extorsion de fonds en échange de données volées semble avoir épargné les entités des Nations Unies jusqu'à ce jour, à quelques exceptions près. Les médias ont rapporté que plusieurs acteurs bien connus, y compris de grandes entreprises du secteur privé et des administrations locales même, avaient été forcées de verser des rançons pour recouvrer l'accès à leurs données et systèmes informatiques. Les Inspecteurs notent qu'à l'heure actuelle, les entités participantes ont clairement pris position contre le paiement de toute rançon à des criminels. Dans le même ordre d'idée, il convient de noter, à ce stade, que les entités des Nations Unies n'ont pas signalé avoir subi de cyberattaques contre des appareils connectés, tels que des ascenseurs, des systèmes de ventilation, des véhicules autonomes ou des équipements similaires télécommandés. Le ciblage d'appareils connectés est certes un aspect naissant des cyberrisques, mais les entités devraient être vigilantes, car les spécialistes du secteur prévoient une augmentation sensible de ce type de menace à l'avenir. Ces deux exemples montrent qu'il importe d'anticiper les risques dont les Nations Unies peuvent n'avoir connu que de rares précédents à ce jour, et d'intégrer des considérations de cybersécurité à titre préventif dans le processus global de gestion des risques des entités.

34. **La cyberassurance.** Les précautions prises contre les menaces naissantes peuvent être étoffées par la souscription d'une cyberassurance. Destinée à couvrir les dommages causés par les cyberattaques, cette solution pourrait aussi être un moyen d'esquiver l'aspect éthique de la question du paiement d'une rançon. Les fournisseurs commerciaux pourraient être requis par leur client, au cas par cas, de fournir une telle couverture. Au cours de l'examen, aucune entité des Nations Unies n'a déclaré s'être assurée contre le risque d'une cyberattaque, bien que certaines aient indiqué avoir envisagé cette possibilité. Ayant pris acte de la position dominante parmi les entités des Nations Unies, les Inspecteurs ne considèrent pas la cyberassurance comme un instrument efficace pour contrecarrer à titre anticipatif les risques liés aux attaques dans la plupart des contextes opérationnels, en particulier parce qu'elle ne constituerait qu'une stratégie d'atténuation partielle visant à réduire au minimum les pertes financières qu'une cyberattaque pourrait causer, sans pour autant apporter de solution aux dommages causés aux opérations ou à la réputation. Il reste que, **de l'avis des Inspecteurs, les directions exécutives ont tout intérêt à se préparer à la possibilité de telles menaces, qui risquent fort de croître à l'avenir.**

D. Dialogue et coopération avec les autorités nationales

35. **Une pratique inégale et hésitante en matière d'information des autorités nationales.** Les entités participantes procèdent de différentes façons lorsqu'il s'agit de porter les incidents de cybersécurité à la connaissance des autorités nationales qui pourraient être en mesure d'enquêter sur les attaques et de prendre des mesures administratives ou judiciaires à leur encontre. Un tiers environ des entités participantes ont dit avoir déclaré des incidents aux forces de l'ordre nationales, mais rares étaient celles qui avaient procédé de façon systématique ou habituelle. La plupart des entités qui ont déclaré avoir eu des échanges avec les autorités nationales sur des questions de cybersécurité par le passé l'avaient fait au cas par cas plutôt qu'en exécution d'une politique institutionnelle ou d'une pratique établie. Bon nombre avaient alors préféré utiliser des relations de travail informelles, réservant les voies formelles aux situations où des attaques d'envergure auraient pu affecter le pays hôte ou la réputation de l'entité. Même lorsque les capacités d'enquête au niveau national auraient pu dépasser et donc utilement compléter les moyens internes − souvent fort limités − de poursuivre les attaquants suspectés, peu d'entités ont évoqué la volonté ou le besoin d'avoir des échanges systématiques formalisés ou renforcés avec les autorités nationales concernant les atteintes à leur cybersécurité. Le constat est donc celui d'un intérêt limité pour la collaboration avec les autorités nationales et d'une préférence pour le maintien du caractère informel et ad hoc d'éventuelles interactions à ce niveau.

36. **Facteurs influençant la pratique des entités.** Divers facteurs peuvent amener des entités à hésiter avant de prendre contact avec les autorités nationales, parmi lesquels leur statut juridique, à savoir les privilèges et immunités dont elles jouissent, en particulier en ce qui concerne la confidentialité et l'inviolabilité de leurs données, qui les protègent de toute interférence de nature législative, exécutive ou judiciaire. Les limites des obligations juridiques qui se rattachent à ce statut sont souvent mal comprises par les praticiens de la cybersécurité. En fait, tandis que les États ont l'obligation de protéger les entités, celles-ci ne sont tenues de coopérer avec les autorités nationales que dans la mesure où cette coopération n'interfère pas avec l'exercice indépendant de leurs fonctions. Cette coopération est par conséquent toujours volontaire. Maintenir cet équilibre peut effectivement constituer un exercice délicat dans la pratique, mais qui ne devrait pas empêcher une coopération volontaire lorsqu'elle est justifiée et que les risques qu'elle pourrait présenter ont été pleinement évalués. En tout état de cause, il n'y a pas d'obligation de déclarer des incidents aux autorités nationales ni de divulguer quelque donnée sensible que ce soit. Les services juridiques sont les mieux à même de conseiller les décideurs à cet égard. Un autre facteur à prendre en considération pour juger de l'opportunité de prendre attache avec les autorités nationales est le degré de maturité du dispositif de cybersécurité du pays hôte, de même que le traitement qu'il réserve aux cyberdélinquants soumis à sa juridiction nationale. Ces préoccupations peuvent prendre plus d'ampleur lorsque des membres du personnel sont impliqués dans l'atteinte à la cybersécurité de leur entité (menaces internes). La procédure d'usage dans ces cas est de lever les privilèges et immunités et de remettre la personne concernée à l'État dont elle a la nationalité, à charge pour celui-ci d'assurer la suite des enquêtes et, le cas échéant,

d'engager des poursuites. C'est un scénario qui reste cependant comparativement rare, surtout pour des faits commis dans la sphère numérique. Depuis 2007, année où des statistiques ont commencé à être produites et publiées, un seul cas d'inconduite déféré aux autorités nationales par le Bureau des affaires juridiques concernait une atteinte à la sécurité de l'information[11]. Outre les considérations exposées ci-dessus, la gravité de l'incident, l'utilité et la probabilité d'une attribution de l'attaque à un auteur donné, la possibilité que des informations confidentielles ou sensibles soient compromises et l'incidence qu'une enquête pourrait avoir sur les activités de l'entité sont les éléments cités le plus souvent comme intervenant dans la décision de saisir ou non les autorités nationales. Certains responsables ont également reconnu que, souvent, la possibilité de rapporter les faits aux autorités nationales était simplement négligée.

37. **Décision d'en référer aux interlocuteurs nationaux.** Comme exposé ci-dessus, la décision de prendre attache ou non avec les autorités nationales touche à des domaines qui ne sont pas de la compétence des spécialistes de la cybersécurité. Entrent en jeu une combinaison de considérations politiques, juridiques, relatives à la preuve et pratiques qui nécessitent l'intervention d'une pluralité de parties prenantes. Dans les entités où les Inspecteurs ont constaté l'existence d'interactions plus rodées avec les autorités nationales, la distribution des responsabilités était à l'image de l'éventail des considérations en jeu, ce qui a été considéré comme une bonne pratique. En termes plus spécifiques, le bureau de programme ou l'unité organique touché évaluait la gravité de l'intrusion, mesurant les risques et les avantages qu'il y aurait à prendre contact avec les autorités nationales. Le bureau juridique procédait à son évaluation et donnait son avis sur les ramifications juridiques possibles étant donné le statut spécial de l'entité et de son personnel, notamment sur la nécessité éventuelle de lever les privilèges et immunités et, le cas échéant, de soumettre le membre du personnel à la juridiction de son pays de nationalité. Le service des TIC ou les spécialistes de la cybersécurité avaient pour rôle de fournir, dans la mesure où elles étaient disponibles, des preuves de la violation. La décision de saisir ou non le pays hôte revenait à la direction exécutive, moyennant la contribution de toutes les parties prenantes susmentionnées. Une fois prise la décision d'informer les autorités nationales d'un incident, les mécanismes pour ce faire étaient normalement les lignes de communication établies entre les bureaux concernés des entités des Nations Unies, la mission permanente de l'État concerné et les autorités compétentes du pays hôte. Au vu de certains commentaires critiquant l'efficacité du processus en place, il pourrait être opportun d'envisager des façons de procéder différentes ou complémentaires, dont certaines sont décrites ailleurs dans le présent rapport (par. 161 à 163).

E. État de préparation technologique et questions appelant examen

38. **La bonne implantation des capacités techniques de base et la mise en évidence de domaines appelant une attention particulière.** Les Inspecteurs ont posé aux entités participantes une série de questions destinées à examiner leur état général de préparation technologique face aux menaces à la cybersécurité. L'intention ce faisant n'était pas de procéder à une évaluation exhaustive de la robustesse de leurs dispositifs opérationnels ou de leur infrastructure technique, mais de prendre la mesure des capacités générales dont elles disposaient et de cerner certaines questions qui mériteraient une attention particulière. Sans perdre de vue les limitations inhérentes aux informations recueillies principalement par auto-évaluation, de même que les variations considérables du degré de précision avec lequel les réponses ont été fournies aux Inspecteurs, il ressort des informations reçues qu'aux yeux des entités participantes, les aspects techniques centraux de la cybersécurité ont été bien compris et ont fait l'objet d'investissements suffisants, eu égard à leurs capacités propres. Ainsi les deux tiers des entités participantes ont-elles indiqué qu'elles disposaient d'outils de surveillance des réseaux. La plupart ont en outre déclaré avoir installé des pare-feu ou d'autres systèmes de prévention des intrusions, et 13 ont dit avoir mis en œuvre un système de gestion des événements et des informations de sécurité. C'est dans les domaines qui ont connu un développement technologique plus dynamique dans un passé récent que le tableau est plus nuancé et mériterait une attention particulière de la part des entités participantes.

[11] A/75/217, annexe I.

Dans le cadre de la présente section, les dispositifs spécifiques aux entités ne sont pas identifiés de sorte à éviter que ne puissent en être dégagées des constatations susceptibles de nuire à la sécurité des entités concernées.

Gestion des appareils finals et outils facilitant le travail à distance

39. **La gestion des appareils finals mise à l'ordre du jour par la pandémie de COVID-19.** La pandémie a forcé la mise en œuvre de nouvelles modalités de travail flexible à une échelle beaucoup plus grande qu'auparavant, pour presque tous les groupes professionnels, tant aux sièges que sur le terrain. Dans ces circonstances, la capacité des entités de fonctionner hors site, en s'accommodant d'un accès réduit aux locaux et au matériel informatique centralement connecté, a été soumise à une épreuve de résistance inédite, et les outils destinés à faciliter le travail à distance font l'objet d'un examen de plus en plus attentif du point de vue de la cybersécurité. Il s'agit, d'une part, de veiller à ce que les employés puissent accéder à distance et en toute sécurité aux ressources informatiques, ce que les deux tiers des entités ont dit faciliter par la mise en service de réseaux privés virtuels, tandis que les autres ont dit recourir à des services en *cloud* (ou en nuage) accessibles par les réseaux publics, moyennant des protocoles Internet cryptés, ce qui les dispensait de monter des réseaux virtuels privés. D'autre part, la capacité de fonctionner hors site requiert une gestion des appareils finals (ordinateurs de table, ordinateurs portables et autres appareils mobiles), dont la prise en charge, selon les réponses, connaît de plus grandes variations.

40. **Les retards dans la gestion des appareils finals.** Bien que la majorité des entités mentionnent un certain degré de gestion centralisée des appareils, plusieurs semblent assurer cette fonction de façon incomplète. Dans certains cas, sa portée est limitée aux appareils du siège, sept entités faisant observer que leurs bureaux locaux disposaient de leurs propres méthodes de gestion des appareils ; dans d'autres cas, seuls les ordinateurs connectés en permanence bénéficiaient d'une gestion centrale, tandis qu'un tiers des entités participantes n'assuraient aucune gestion ni protection centrale des appareils mobiles, même si quelques-unes s'attachaient ou s'apprêtaient à mettre en place des plateformes à cette fin. Seules deux réponses font état du cryptage des appareils finals, mesure pourtant importante pour prévenir le vol et la fuite de données, en particulier dans le cas des appareils portables des utilisateurs finals, qui sont généralement plus exposés aux pertes et aux vols. Il ressort des réponses que si les entités étaient conscientes de la nécessité d'une prise en charge au niveau institutionnel, la gestion des appareils mobiles restait en retrait. Les vulnérabilités existantes à cet égard étaient exacerbées par l'utilisation d'appareils mobiles personnels qui ne relevaient pas de l'entité, tels que des ordinateurs portables privés − une pratique qui a connu un essor considérable pendant la pandémie.

41. **L'adoption ou la mise en place accélérée d'importantes mesures de cybersécurité.** Malgré tous les problèmes qu'elle a causés, la pandémie a aussi été l'occasion d'évolutions positives. Les entités des Nations Unies ont été amenées à se pencher de plus près sur leurs cadres de gestion de la sécurité. Des projets institutionnels relatifs aux TIC ont commencé à se concrétiser pour répondre à des besoins immédiats. On peut dire que la migration massive et à brève échéance vers le travail à distance a conduit de nombreuses entités à renforcer d'urgence la sécurité de leurs accès à distance et qu'à en juger par les réponses faites aux questionnaires du CCI, elle aurait donné une impulsion longtemps espérée pour dynamiser l'action dans ce domaine. De fait, la plupart des entités ont mis en place des systèmes d'authentification multifactorielle pour sécuriser leurs accès à distance, déployé des outils de collaboration et de partage des données en ligne à un niveau sans précédent, poussé plus loin encore l'institutionnalisation de la signature électronique et rendu plus nombreuses les occasions de formation à la sécurité de l'information. Dans un sens, la pandémie est devenue un catalyseur pour la transformation des outils informatiques et de communication de plusieurs entités des Nations Unies, encouragées sur la voie de la transformation numérique et des formes avancées de travail numérique − une évolution qui a des implications non seulement pour la cybersécurité, mais aussi, de façon beaucoup plus large, pour la manière dont les entités fonctionnent et gèrent leurs actifs et leurs locaux.

Systèmes informatiques préexistants

42. **Vulnérabilités propres aux systèmes informatiques préexistants.** Plusieurs entités participantes ont relevé que l'actualisation ou le retrait des systèmes informatiques vieillissants qui pourraient ne plus être compatibles avec les applications les plus avancées représentaient des défis de taille pour la cybersécurité. Le maintien de ces systèmes préexistants a été décrit comme une importante source de vulnérabilités, car bon nombre avaient été conçus pour un usage local, dans le cadre de réseaux privés − locaux ou étendus − considérés à l'époque comme sûrs. C'est principalement en raison du développement de l'accès à distance et de l'informatique en nuage que ces applications sont aujourd'hui beaucoup plus exposées aux risques afférents à l'interconnectivité généralisée des systèmes et des données, sans compter qu'elles n'ont pas été conçues pour résister à des formes d'attaques plus contemporaines. Si certaines des failles ainsi créées peuvent être enregistrées et signalées par les systèmes de gestion des vulnérabilités, il reste possible que certaines des applications propriétaires encore en place ne soient pas balayées automatiquement et que, même en cas de balayage, les corrections voulues se fassent attendre, ce qui prolonge outre mesure l'exposition au danger des entités concernées. Aux risques propres aux applications existantes elles-mêmes, s'ajoute le fait que leurs points faibles peuvent aussi mettre en danger d'autres applications et données qui reposent sur les mêmes infrastructures, car les premières, une fois compromises, peuvent servir à effectuer des déplacements latéraux entre les systèmes ou les applications, et compromettre ainsi les secondes.

43. **L'importance d'un examen attentif des systèmes préexistants.** Il importe par conséquent que les entités des Nations Unies tiennent un relevé de leurs systèmes plus anciens et qu'elles s'emploient activement à les actualiser ou à les remplacer. Sachant que certains d'entre eux sont grands et complexes (comme les progiciels de gestion intégrés) et qu'ils sont nombreux à avoir été mis au point au fil des ans au sein même des entités et selon leurs besoins particuliers, c'est une tâche qui peut s'avérer complexe dans bien des cas, et requérir des ressources financières supplémentaires de même que des efforts particuliers pour obtenir et maintenir l'adhésion des unités administratives qui avaient investi dans la mise au point des solutions sur mesure aujourd'hui considérées comme peu sûres. **Les Inspecteurs proposent que les chefs de secrétariat, en étroite collaboration avec des spécialistes des TIC et de la cybersécurité, ainsi que les unités administratives affectées, entreprennent, si ce n'est déjà fait, un examen attentif de la question des systèmes préexistants au sein de leur entité.** Les considérations de cybersécurité devraient figurer en bonne place dans cette analyse, au même titre que la considération stratégique et opportune des implications en matière de ressources et des effets immédiats et à long terme sur les opérations de la mise hors service des systèmes visés, lesquels devraient faire l'objet d'une planification adéquate en vue de l'instauration de mesures d'atténuation temporaires, lorsque cela est possible.

Sécurité de l'informatique en *cloud* (ou en nuage)

44. **Une amélioration considérable, selon la communauté des spécialistes de la cybersécurité, de la protection offerte par les fournisseurs de services d'informatique en *cloud*.** Depuis 2019, lorsque le CCI a publié son rapport sur l'informatique en *cloud* ou en nuage[12], tant l'utilisation de cette formule par les entités participantes que sa portée et sa maturité ont connu une expansion considérable. Sa versatilité, son élasticité (qui lui permet d'adapter en continu et en temps réel l'allocation de ressources informatiques à la demande effective), sa rentabilité et son perfectionnement technologique sans cesse croissant ont suscité la confiance des utilisateurs dans sa robustesse et sa sûreté, la rendant d'autant plus attrayante aux yeux du système des Nations Unies. Les entités continuent de transférer leurs applications existantes vers des services en *cloud*, les décisions prises à ce sujet restant propres à chacune. À cet égard, les Inspecteurs prennent acte du fait que les membres de la communauté des spécialistes de la cybersécurité sont toujours plus nombreux à considérer que les capacités et les garanties informatiques proposées par les leaders du secteur commercial dépassent aujourd'hui le niveau de sécurité, de confidentialité et de cyberrésilience qu'ils pouvaient offrir il y a à peine un an ou deux. Toujours selon les spécialistes, tout indique par ailleurs que les protections actuellement garanties par ces

[12] JIU/REP/2019/5.

fournisseurs dépassent le niveau de sécurité que n'importe quelle entité serait capable d'atteindre au moyen de ses propres solutions de sécurité. Selon le présent examen, une seule entité a choisi d'exclure complètement du *cloud* ou du nuage une portion précise, particulièrement sensible, des données dont elle avait la responsabilité. À noter toutefois que cette mesure a été prise pour un ensemble limité de données et compte tenu de la capacité de l'entité en question − notamment sa capacité financière − d'assurer une solution de remplacement viable, ce qui est hors de portée de la plupart des entités.

45. **La nécessité d'une vigilance soutenue lorsque sont utilisés des services externes d'informatique en *cloud* (ou en nuage).** Même si la sécurité de l'informatique en *cloud* a fait de grands progrès ces dernières années, les recommandations adressées aux chefs de secrétariat dans le cadre du rapport du CCI susmentionné restent valables dans les cas suivants : veiller à ce que les services d'informatique en *cloud* soient conformes aux besoins de l'entité pour obtenir un bon retour sur investissement ; procéder à une analyse exhaustive des risques et une gestion attentive des fournisseurs avant d'externaliser des services d'informatique en nuage ; adopter des stratégies visant à atténuer le risque que des fournisseurs soient dans l'incapacité de fournir les services contractuels. Des préoccupations subsistent également concernant la monopolisation et la concentration excessive de données des Nations Unies aux mains d'un nombre relativement peu élevé de géants de la technologie. Les entités ne peuvent donc pas se permettre de relâcher leur vigilance lorsqu'elles utilisent des applications en *cloud* ou y mettent leurs propres applications et données, surtout eu égard au risque que des données confidentielles ou sensibles soient obtenues sans autorisation. Elles doivent continuer de faire preuve de la diligence voulue et de suivre les bonnes pratiques de cybersécurité lorsqu'elles s'appuient sur des services d'informatique en *cloud*, notamment en vérifiant que le fournisseur remplit les conditions d'audit indépendant et dispose des certifications pertinentes, tels les rapports « *System and Organization Controls* » ou « *SOC* », en particulier les rapports « *SOC 2* », ou de garanties similaires largement reconnues par les spécialistes du secteur. Exiger de telles garanties externes et indépendantes devient important dès lors que sont engagés des fournisseurs externes et que les mécanismes d'audit interne et d'autres mécanismes de contrôle institutionnel peuvent ne plus trouver à s'appliquer. Il est par conséquent recommandé d'obtenir l'avis du service d'audit interne lorsqu'il est question de passer des contrats pour la fourniture de tels services, de sorte que soient incluses les dispositions nécessaires pour disposer de garanties raisonnables de conformité avec les normes pertinentes de contrôle interne en matière de collecte, de stockage et d'utilisation de l'information fournie. La consultation du bureau juridique est aussi souhaitable. Les entités doivent en effet trouver des moyens acceptables d'exercer un contrôle jugé suffisant sur les services fournis, par exemple en incluant dans leurs contrats avec des fournisseurs de services d'informatique en *cloud* des clauses qui leur permettent de surveiller et de vérifier la conformité. Il se peut, par ailleurs, que des installations commerciales d'informatique en *cloud* changent de propriétaire, y compris d'un pays à un autre, ce qui pourrait, dans certaines circonstances, exacerber le risque d'exposition des données stockées ou gérées par de telles facilités en cas d'action en justice intentée sous la juridiction nationale concernée. Dans une telle situation, les privilèges et immunités seraient affirmés et maintenus pour toutes les données détenues pour le compte des entités des Nations Unies. Cela étant, les entités doivent rester vigilantes et prendre les précautions voulues pour gérer de tels risques autant que faire se peut.

46. **L'impossibilité du risque zéro et la nécessité d'une analyse détaillée.** Indépendamment des gains de rentabilité et de sécurité à réaliser, les Inspecteurs rappellent que les menaces à la cybersécurité existent pour l'informatique en *cloud* (ou en nuage) comme pour la formule traditionnelle des centres de données, et que ni l'une ni l'autre ne peut prétendre à l'impénétrabilité. Dans un cas comme dans l'autre, l'élimination complète des risques n'est pas un projet réaliste. Lorsque ces risques sont, dans une certaine mesure, transférés à des entités externes chargées de gérer tel ou tel aspect d'un environnement informatique, les conséquences d'une cyberattaque restent une responsabilité interne. Les entités ont donc tout intérêt à se livrer à une analyse détaillée avant de décider si et, le cas échéant, dans quelle mesure, elles sont disposées à confier la protection de leur information à une tierce partie. À cet égard, les évaluations de la protection des données devraient vérifier que les garanties offertes par les services d'informatique en *cloud* correspondent aux exigences de l'entité ainsi qu'à la nature et au caractère sensible des

ensembles de données concernés. Des précautions similaires valent pour toute décision de sous-traitance et ne concernent pas seulement le recours à la sécurité de l'informatique en *cloud*.

Gestion des vulnérabilités

47. **Les pratiques sont inégales parmi les entités participantes.** Aujourd'hui, la gestion des vulnérabilités est considérée comme l'un des principaux défis de la cybersécurité des organisations internationales. De nouvelles vulnérabilités affectant des logiciels largement utilisés, dont les logiciels utilisés par les entités des Nations Unies, sont découvertes presque tous les jours. Des correctifs sont constamment mis au point et à disposition par les fournisseurs de matériels et de logiciels, mais ces modifications représentent un volume considérable d'informations à traiter et leur application dans des environnements d'une grande complexité technique entraîne une lourde charge de travail. Plus de la moitié des entités participantes ont déclaré qu'elles disposaient, pour relever ce défi, d'une forme de gestion des vulnérabilités. Ainsi certaines s'abonnent-elles à des fils de renseignements pour se tenir constamment au courant des nouvelles menaces, y compris des nouvelles vulnérabilités (et s'en protéger), tandis que d'autres ont choisi de mettre en place des solutions de sécurité intégrées, notamment de gestion des vulnérabilités, obtenues auprès de fournisseurs commerciaux. La détection et la correction des vulnérabilités a été qualifiée par certaines entités d'activité exigeante. Certaines ont relevé que les tentatives malveillantes de déceler des vulnérabilités dans leurs réseaux et systèmes se faisaient plus nombreuses avec le temps, alors que la nature distribuée de leurs réseaux informatiques et de communication rendait problématique la gestion centralisée du processus de correction des vulnérabilités, en particulier lorsqu'il fallait compter avec de multiples sites locaux. Plusieurs entités ont aussi signalé que les dépenses occasionnées par les corrections figuraient parmi les postes les plus importants de leurs programmes de cybersécurité .

48. **La nécessité d'une gestion continue de la cybersécurité.** Les Inspecteurs attirent l'attention sur le grand écart d'efficacité entre une évaluation ponctuelle (annuelle, par exemple) et un processus continu de gestion et de correction des vulnérabilités. À défaut d'une application régulière des corrections, les systèmes informatiques restent trop longtemps ouverts aux exploitations, le risque de piratage augmentant considérablement. Les informations recueillies auprès des entités participantes à ce sujet ne permettent pas d'affirmer que les entités s'occupaient de ce problème de façon suffisante et conséquente. Les réponses faites au questionnaire du CCI par plusieurs d'entre elles donnent plutôt à voir une approche plus ponctuelle des évaluations des vulnérabilités (effectuées annuellement, voire moins souvent), tandis que d'autres, comme l'Office de secours et de travaux des Nations Unies pour les réfugiés de Palestine dans le Proche-Orient (UNRWA), le Programme alimentaire mondial (PAM), l'OACI et l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) comptent la gestion efficace et continue des vulnérabilités parmi les bonnes pratiques dans leurs entités. **Considérant qu'il y a matière à amélioration dans ce domaine, les Inspecteurs recommandent vivement aux chefs de secrétariat d'accorder une attention et des ressources suffisantes à la conduite d'évaluations régularisées des vulnérabilités, de sorte que la gestion de ces dernières devienne une activité systématique au sein des entités des Nations Unies.**

Informatique fantôme

49. **Les raisons du recours à l'informatique fantôme.** L'expression « informatique fantôme » (*Shadow IT*) renvoie à des applications ou des solutions informatiques mises au point ou adoptées au sein d'une entité, mais en dehors de son cadre informatique officiel dont la gestion est habituellement centralisée. Le plus souvent, l'informatique fantôme est le fait d'utilisateurs qui tentent de résoudre un problème pratique en se servant d'outils directement disponibles sur le marché, à faible prix ou gratuitement, parce que les solutions disponibles par les canaux établis et les capacités informatiques structurées ne leur paraissent pas répondre à leurs besoins pour ce qui concerne les délais, les coûts ou les possibilités d'adaptation. Elle peut aussi résulter d'une volonté d'innover rapidement pour suivre l'évolution des besoins ou d'assurer l'alignement ou la compatibilité avec des outils qui sont utilisés par des partenaires d'exécution, mais qui ne correspondent pas au choix retenu par l'entité au niveau institutionnel. Il s'agit par exemple de l'ouverture de comptes gratuits

auprès de fournisseurs de services qui proposent des solutions de stockage des données, de transfert de fichiers, de conception de sites Web et de gestion de contenus Web, ou de la mise au point d'applications maison à l'usage de certains services, bureaux locaux ou projets. La conformité de ces solutions aux règles et procédures de cybersécurité mises en place par l'autorité officielle et centralisée, au niveau de l'entité, n'est pas normalement ou nécessairement vérifiée, de sorte qu'elles peuvent être considérées comme fonctionnant dans un environnement « fantôme », non autorisé.

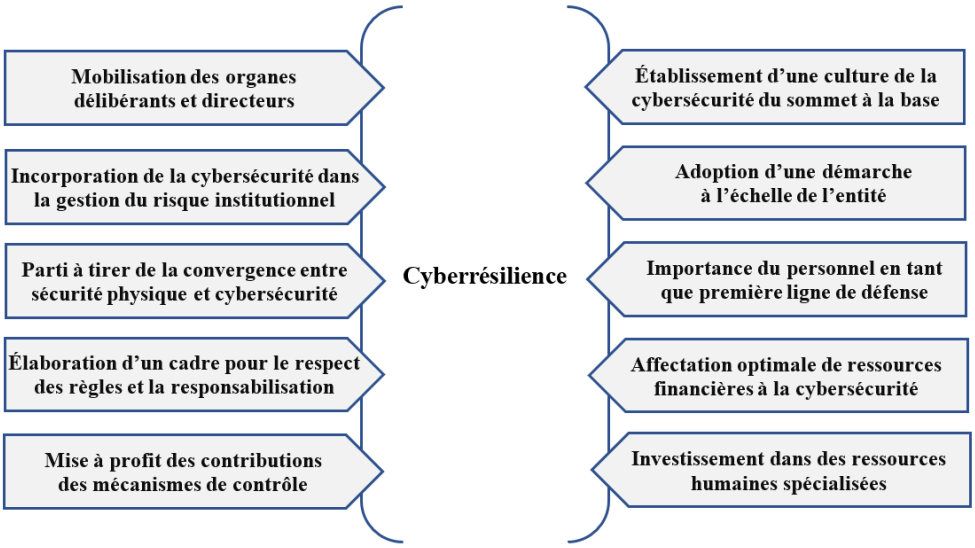
50. **Les risques afférents à l'utilisation de l'informatique fantôme.** La prolifération du phénomène a été évoquée en rapport plus particulièrement avec des bureaux locaux ou des services éloignés, d'une façon ou d'une autre, du contrôle central. Les risques dans ces situations sont souvent amplifiés par le fait que les départements centraux de l'informatique et de la cybersécurité ont moins la possibilité de se faire une idée des activités de développement informatique qui y sont entreprises. À cela s'ajoute derechef le fait que la pandémie de COVID-19, en rendant pressante la réalisation de multiples tâches à distance, est venue accentuer cette tendance, amenant de nombreux utilisateurs à adopter des outils de collaboration en ligne, notamment de visioconférence, en marge des solutions fournies dans le cadre des progiciels institutionnels. Un grand nombre des services de remplacement auxquels les utilisateurs ont fait appel n'avaient pas été évalués et autorisés par les spécialistes de la cybersécurité des entités, faisant ainsi courir des risques à ces dernières (notamment en pratiquant des normes différentes de celles recommandées au niveau de l'entité en matière d'authentification et de confidentialité). À titre d'exemple, à l'issue de l'étude que le Groupe d'intérêt pour la sécurité informatique a faite, aux premiers temps de la pandémie, d'une certaine plateforme de visioconférence populaire, afin d'en déterminer l'adéquation à un usage éventuel par les entités des Nations Unies, les spécialistes de la cybersécurité ne sont pas parvenus à rendre une recommandation définitive et univoque − positive ou négative − qui puisse être considérée comme valable pour le système dans son ensemble. Ils ont dû se résoudre à formuler une série de possibilités assorties de mises en garde et de précautions à considérer avant d'utiliser la plateforme dans des situations spécifiques.

51. **Des propositions tendant à une gestion plus vigilante de l'informatique fantôme. Les Inspecteurs considèrent que les difficultés en matière de cybersécurité créées par la pratique de l'informatique fantôme méritent plus d'attention, s'agissant d'équilibrer la nécessité d'exercer un contrôle sur un environnement propice aux cyberrisques, d'une part, et les besoins légitimes ainsi que la motivation constructive qui amènent les utilisateurs à innover et à rechercher des solutions de remplacement, d'autre part.** En fait, la conclusion qui s'est dégagée est qu'il ne faut pas rejeter d'emblée comme indésirable l'impulsion qu'ont certains utilisateurs de se tourner vers l'informatique fantôme, mais y voir aussi la manifestation bienvenue d'une volonté d'innover à laquelle les unités administratives devraient généralement pouvoir accorder une place et consacrer des ressources, idéalement dans un environnement informatique protégé. Les idées suivantes sont exploitables à cette fin : créer des environnements sûrs pour l'innovation informatique ou étendre ceux qui existent déjà ; rendre plus visibles, par l'entremise de points de contact locaux pour les TIC, les activités de développement distribué menées dans les sites décentralisés ; renforcer la formation des utilisateurs finals et les mesures de sensibilisation afin d'y inclure des informations fiables et claires sur les questions de sécurité et les risques afférents à l'utilisation de services externes en dehors des procédures et pratiques standard, en même temps que sur la disponibilité de solutions internes dûment approuvées, ainsi que des recommandations en vue d'un usage plus sûr des services externes.

III. Facteurs d'amélioration de la cyberrésilience

52. **La conception de la cyberrésilience en tant que corollaire de la cybersécurité**. Outre la préparation technologique, notamment la désignation de solutions numériques et de sources de données aux fins de la protection des ressources institutionnelles, un dispositif de cybersécurité robuste s'appuie sur une approche à plusieurs facettes qui mobilise tous les niveaux de l'entité, y compris les organes délibérants et directeurs, les mécanismes de contrôle, la direction exécutive, les unités organiques et administratives et les directeurs de programme, le personnel dans son ensemble, de même que les partenaires d'exécution et les fournisseurs de services externes. En d'autres mots, une approche globale, au niveau de toute l'entité, est indispensable pour créer les conditions nécessaires à l'amélioration de sa cyberrésilience. En plus, la cybersécurité recoupe plusieurs domaines et compétences, notamment les TIC, la gestion des risques, la sûreté et la sécurité physiques et, plus largement, la gestion de l'information et des connaissances. La multiplicité des facteurs à considérer et la conscience qu'ont les parties prenantes du rôle qu'elles ont à jouer et de la contribution qu'elles ont à apporter pour élever le niveau de cybersécurité de chaque entité peuvent être considérées comme les composants d'une culture de la cybersécurité qui, une fois instaurée et mise en pratique, concourt à la réalisation de la résilience de l'entité. Dans ce chapitre, les Inspecteurs exposent leurs constatations quant à la mesure dans laquelle les cadres et les pratiques des entités participantes présentent ces facteurs qui contribuent à une plus grande cyberrésilience (selon la perspective verticale), comme résumé dans la figure IV. Ils proposent des améliorations possibles.

Figure IV
Facteurs d'amélioration de la cyberrésilience



Source : Établi par le CCI.

Note : Aux termes d'une des grandes normes du secteur, la cybersécurité s'entend de la capacité d'un système qui use ou dépend de cyberressources d'anticiper les circonstances adverses, les épreuves, les attaques ou les atteintes qui le menacent, d'y résister, de s'en remettre et de s'y adapter.

A. Mobilisation des organes délibérants et directeurs

Orientations stratégiques et ressources à fournir par les organes délibérants et directeurs

53. **L'importance de l'attention portée à la cybersécurité par les organes délibérants et directeurs.** Le CCI a toujours déclaré que les organes délibérants et directeurs des entités intergouvernementales ont pour rôle décisif de fournir les orientations stratégiques et les ressources dont toute entité a besoin pour exécuter les tâches relevant de son mandat. Comme indiqué dans un récent rapport du CCI sur la gestion du risque institutionnel[13], les organes

[13] JIU/REP/2020/5.

délibérants et directeurs doivent participer à la gestion des risques et doivent, au minimum, connaître les principaux risques stratégiques auxquels une entité fait face, ainsi que les stratégies et cadres qui existent pour les gérer. **De l'avis des Inspecteurs, cette exigence de participation et d'orientation devrait s'étendre au domaine de la cybersécurité qui constitue un enjeu crucial à la fois pour la gestion des risques et pour l'exécution du mandat des entités.** Des moyens concrets par lesquels les organes concernés peuvent accroître leur participation et soutenir les efforts de l'entité dans le domaine de la cybersécurité sont proposés dans l'encadré 3. Cela étant, étant donné que la cybersécurité continue d'être perçue comme une question essentiellement technique et, partant, d'ordre opérationnel plutôt que stratégique, la mesure dans laquelle les organes délibérants et directeurs ont été appelés, ou ont eux-mêmes demandé, à s'investir dans la question est restée modeste dans la plupart des entités.

Encadré 3
Possibilités pour les organes délibérants et directeurs de s'investir dans la cybersécurité

- Formuler une déclaration explicite portant sur la tolérance au risque et l'appétit pour le risque de l'entité dans le domaine de la cybersécurité, et sur le degré de risque considéré comme acceptable dans ce contexte. Il n'a guère été question de telles déclarations parmi les entités participantes, exception faite du Programme des Nations Unies pour le développement (PNUD) et de l'Organisation internationale de la propriété intellectuelle (OMPI), où existe une méthode sophistiquée et bien conçue d'expression de l'appétit pour le risque.
- Fournir une orientation stratégique de haut niveau concernant les domaines prioritaires de la cybersécurité. Un bon exemple d'une telle orientation se trouve sous le titre « Sécurité des systèmes informatiques » de la stratégie informatique et communications du Secrétariat de l'ONU, approuvée par l'Assemblée générale en 2014 (A/69/517).
- Allouer, sur la base d'un solide dossier de décision présenté par la direction exécutive, les ressources financières nécessaires à la réalisation des objectifs définis dans le cadre de l'orientation stratégique établie par les organes délibérants et directeurs en fonction de l'appétit pour le risque.

54. **La participation effective des organes délibérants et directeurs.** La collaboration avec les organes délibérants et directeurs est variable, se faisant plus ou moins étroite et étendue en fonction, principalement, du mandat et des besoins opérationnels des entités. Elles étaient peu nombreuses à reconnaître − et encore moins à exploiter − les avantages d'une mobilisation des organes délibérants et directeurs en faveur de la cybersécurité. Dans la plupart des cas, cette reconnaissance avait été la conséquence d'une attaque de grande envergure qui avait nécessité un supplément d'attention et amorcé une interaction au niveau des organes supérieurs. Celle-ci pouvait se présenter sous diverses formes, sans qu'il soit nécessaire de parler d'un seul « bon » degré d'interaction. De fait, il est d'ores et déjà admis que l'existence d'un flux d'information, quel qu'il soit, entre les membres d'une entité et les responsables de sa cybersécurité, n'est pas seulement bénéfique, mais aussi nécessaire. Ci-après, les Inspecteurs établissent la distinction entre les mécanismes ordinaires de communication de l'information dans le domaine de la cybersécurité et les procédures à suivre pour faire remonter l'information aux organes délibérants et directeurs en cas d'incident.

Mécanismes de communication et de remontée de l'information

55. **Les mécanismes existants de communication de l'information.** Les Inspecteurs ont constaté qu'une minorité d'entités informaient périodiquement leurs organes délibérants et directeurs de l'état de leur cybersécurité. Lorsqu'il existe, ce type de communication prend différentes formes : a) certaines entités font figurer l'information en question dans leur budget-programme et leurs rapports sur l'exécution du budget (habituellement sous le chapitre consacré aux TIC, qui peut ou non s'étendre explicitement à la cybersécurité) ; b) d'autres établissent des rapports particuliers, lorsque leurs organes délibérants et directeurs

le demandent et qu'il convient de rendre compte, par exemple, de la mise en œuvre d'une stratégie ou d'une feuille de route cautionnées ou adoptées ; c) d'autres encore s'appuient sur les rapports annuels de leurs organes de contrôle internes, qu'ils utilisent comme principal canal pour insister sur l'attention accrue que mérite la question.

56. **L'absence de collecte et de présentation systématique des indicateurs de cybersécurité.** Des disparités existent également quant au contenu de l'information qui est communiquée aux organes délibérants et directeurs. Les entités qui partagent certains aspects des indicateurs d'exposition et de performance dont elles assurent la collecte et l'analyse en rapport avec la cybersécurité ne sont pas nombreuses. Ces variations dans la communication de l'information peuvent s'expliquer, d'une part, par une réticence légitime de nombreuses entités qui craignent que la présentation des relevés publics ou même classifiés de leurs indicateurs de cybersécurité ne mette en évidence leurs vulnérabilités et ne les expose à des risques supplémentaires, et d'autre part, par les difficultés que les entités peuvent encore éprouver à déterminer le degré de détail et les critères de sélection selon lesquels elles doivent présenter leurs indicateurs, ou encore les indicateurs les plus importants à retenir au départ. La majorité des entités participantes mesurent principalement, à des fins internes, la fréquence, la gravité et le volume des atteintes à la cybersécurité relatifs à une période donnée, certaines devant encore instaurer ou formaliser des formes plus adaptées de collecte des données dans ce domaine. Il reste que le type de données collectées et analysées varie grandement d'une entité à l'autre, et que la façon dont elles sont traitées pour éclairer la prise de décisions, au niveau interne ou à celui des organes délibérants et directeurs, doit encore être définie dans bon nombre d'entités. Dès lors que ces indicateurs sont un des principaux éléments sur la base desquels une entité peut concevoir et énoncer son appétit pour le risque, **les Inspecteurs considèrent qu'il est prudent de poursuivre, dans les sphères concernées, l'étude de différents ensembles d'indicateurs de cybersécurité et de mettre au point une méthodologie de base qui puisse être adaptée, selon les besoins, au contexte de chaque entité**.

57. **La remontée de l'information vers les organes délibérants et directeurs et les avantages de la transparence.** Les réponses faites au questionnaire du CCI par les entités participantes font clairement ressortir qu'en cas d'atteinte à la cybersécurité, les organes délibérants et directeurs ne sont pas systématiquement informés. Les Inspecteurs ont en outre constaté qu'il n'était guère question de processus prédéfinis pour la remontée de l'information vers les organes délibérants et directeurs dans cette éventualité. La décision de faire remonter l'information est habituellement prise au cas par cas. L'expérience des entités qui, souvent forcées par des faits majeurs affectant leur cybersécurité, ont eu l'occasion de mettre à l'épreuve les canaux de remontée et de communication dont elles disposaient pour informer leurs organes directeurs, met en exergue comme suit les principaux facteurs à considérer pour décider de l'opportunité de faire remonter l'information : a) la gravité de l'atteinte ; b) son incidence sur les opérations ; c) son incidence sur les processus intergouvernementaux ; d) la possibilité qu'il devienne public. Sont également décisifs le moment choisi pour faire remonter l'information et les précautions prises pour ne pas révéler certaines vulnérabilités ou certains détails de la capacité de riposte de l'entité, qui pourraient davantage attirer l'attention sur la cible. Les spécialistes de la cybercriminalité interrogés estimaient dans l'ensemble qu'il était bon d'informer les organes supérieurs avant la résolution complète de l'incident, ou plutôt dès que le problème avait été suffisamment cerné, car une remontée dès la découverte de l'intrusion pouvait s'avérer prématurée, compromettre les efforts de résolution en cours et, partant, aggraver le risque. Cela étant, le parti d'attendre que l'incident soit complètement résolu pour en informer les organes supérieurs peut jeter le doute sur la fiabilité de la direction exécutive ou sur sa volonté d'agir avec transparence et d'endosser la responsabilité d'éventuelles défaillances de la cybersécurité. L'idée générale qu'ont fait passer les entités participantes qui s'étaient « ouvertes » de leurs incidents et défaillances de cybersécurité à leurs organes délibérants et directeurs était de ne pas avoir peur de communiquer parce que le coût mesuré en perte de réputation et en perte de confiance de la part des États donateurs dépasse de loin l'embarras et les retombées négatives − y compris les retombées financières indirectes − que peuvent causer une attaque.

58. **La nécessité, pour les entités comme pour leurs organes délibérants et directeurs, de prévoir des protocoles de remontée de l'information. De l'avis des Inspecteurs, il est important de définir par avance le mécanisme par lequel les organes délibérants et directeurs seront saisis d'une cyberattaque d'une certaine importance.** Dès lors que la

probabilité de telles attaques peut être anticipée, il en est de même du protocole de remontée de l'information qui les concerne. Plus concrètement, le processus concerné, à savoir les critères qui déclenchent la remontée et le dispositif qui détermine qui prend quelles mesures dans quel ordre et avec les éléments provenant de quelle source, ne doit pas être l'affaire d'une décision a posteriori. Livrée à l'improvisation, celle-ci risque plus d'être prise sous la pression des mesures de circonstance à prendre pour limiter les dégâts qu'en suivant dans l'ensemble un protocole établi tout en restant libre de gérer les inévitables variables propres à chaque cas. Qui plus est, le fait de devoir concevoir de telles mesures en mode de crise rend le processus plus vulnérable aux influences indues, dans des circonstances qui sont déjà complexes et potentiellement politisées, alors qu'une situation peut être évitée, dans une large mesure, par l'adoption d'une démarche anticipative. Enfin, et sans remettre en question les protocoles de remontée de l'information élaborés au sein des entités, il pourrait être raisonnable pour les organes délibérants et directeurs de consacrer une discussion à leurs propres règles d'engagement en la matière, en prévision de situations où de graves cas de cyberattaques leur seraient soumis pour délibération et suite à donner. Cette démarche prospective pourrait contribuer à fixer des limites soigneusement étudiées et convenues à l'intervention des organes délibérants et directeurs, de sorte à favoriser un processus décisionnel dépolitisé et de qualité dans un domaine qui peut s'avérer sensible.

B. Incorporation de la cybersécurité dans la gestion du risque institutionnel

59. **Les avantages de la cybersécurité considérée sous l'angle de la gestion des risques.** Selon un récent rapport du CCI, la gestion du risque institutionnel s'entend d'un processus intégré, structuré et continu de définition, d'analyse, d'évaluation, de gestion et de surveillance des risques à l'échelle de l'entité et dans l'intérêt de la réalisation des objectifs de celle-ci[14]. Les fonctions de base qui lui sont associées (habituellement l'identification, la prévention, la détection, la riposte et la reprise, combinées selon des rapports variables) sont à l'image des principaux stades et objectifs de la gestion du risque. Le parti de traiter la cybersécurité comme une composante de la gestion des risques à l'échelle de l'entité présente aussi des avantages pratiques. Présentée comme un enjeu stratégique au niveau institutionnel, elle touche toutes les unités administratives et tout le personnel. Sous cette forme, elle encourage et soutient une démarche et une adhésion globales, à l'échelle de l'entité, fondée sur une prise en charge distribuée des risques. **En outre, les Inspecteurs affirment que l'incorporation formelle de la cybersécurité dans le cadre institutionnel de gestion des risques contribue à élever le rang de la question parmi les diverses priorités de l'entité, tout en fournissant un point de repère officiel au regard duquel les organes délibérants et directeurs et l'équipe de direction peuvent, de concert, décider de la voie à suivre pour gérer au mieux les risques majeurs.** Par ailleurs, comme ces cadres sont le plus souvent conceptualisés sous la forme de documents évolutifs, leurs mesures d'atténuation des risques peuvent être réexaminées et adaptées de façon systématique et répétée pour suivre l'évolution rapide des besoins de l'entité.

60. **Le modèle fondé sur la gestion des risques d'ores et déjà partiellement reconnu.** L'utilité de concevoir la cybersécurité sous l'angle de la gestion du risque a déjà été reconnue de diverses façons, même si les implications pratiques de cette perspective doivent encore être pleinement comprises et absorbées dans de nombreux secteurs du système. Par exemple, dans les comptes rendus de récents symposiums du Groupe d'intérêt pour la sécurité informatique réunissant des spécialistes de la cybersécurité, plusieurs points de l'ordre du jour touchaient à la gestion des risques. Les membres du Groupe d'intérêt ont notamment été appelés à intervenir auprès des représentants de leurs entités au sein du Forum de gestion des risques du Comité de haut niveau sur la gestion pour que les cyberrisques soient inclus dans les points de vue soumis au Forum aux fins de la réalisation de son modèle de maturité de la gestion des risques[15]. La nécessité d'inclure une composante de cybersécurité dans les cadres plus larges que sont la gestion du risque institutionnel et la continuité des opérations a également été soulignée par les comités d'audit et de contrôle de plusieurs entités. En fait, la

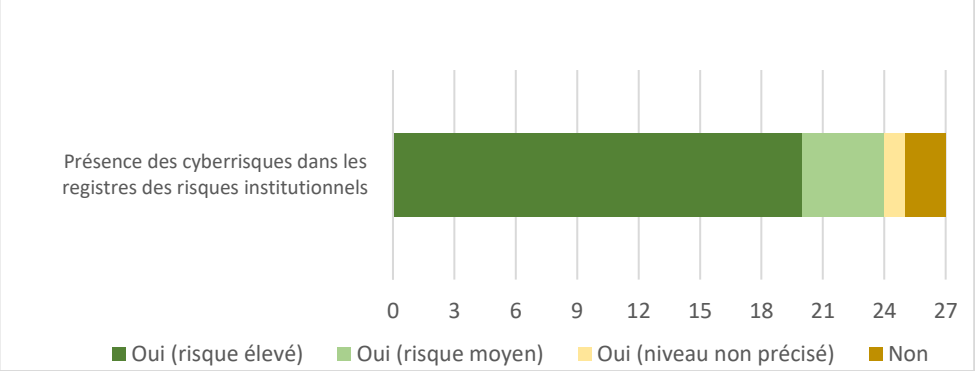
[14] JIU/REP/2020/5.

[15] CEB/2019/HLCM/DTN/02 (en anglais).

plupart de ces comités s'intéressaient à la cybersécurité dans le cadre de leur mandat relatif à la gestion du risque institutionnel des entités, insistant à cet égard sur la plus grande intégration requise entre les fonctions relatives aux TIC et celles qui concernent la gestion des risques. En outre, les normes les plus avancées en matière de cybersécurité, notamment la norme ISO 27001, les Objectifs de contrôle de l'information et des technologies associées, et le cadre du National Institute of Standards and Technology (États-Unis), traitent les cyberrisques comme des risques opérationnels, d'une portée dépassant de loin l'infrastructure informatique, l'accent étant mis sur l'intérêt stratégique qu'il y a à améliorer les dispositifs de cybersécurité des entités et à le faire, pour obtenir les meilleurs résultats, en totale corrélation avec la gestion des risques au niveau de l'entité.

61. **L'attention portée à la gestion des risques dans les entités participantes.** La mesure dans laquelle la cybersécurité a trouvé sa place parmi les questions de gestion des risques connaît des variations. Dans leurs réponses, la grande majorité des entités participantes étudiées par le CCI (24 sur 27) ont déclaré que les risques relevant de la cybersécurité avaient été officiellement inclus dans leur registre des risques institutionnels. Vingt d'entre elles ont indiqué qu'un niveau de risque « élevé » leur avait été attribué (fig. V), et 19 avaient prévu des mesures d'atténuation des cyberrisques dans leur registre. Seules 11 entités participantes ont fourni aux Inspecteurs des documents internes concernant leur gestion des risques, dans lesquels elles partageaient confidentiellement des extraits de leur registre. Étant donné la nature incomplète de cet ensemble de données, les conclusions dégagées doivent être considérées comme préliminaires. La comparaison de certains de ces échantillons fait toutefois apparaître certaines différences dans la manière dont les cyberrisques sont évalués et catégorisés, ainsi que dans la planification les concernant. D'un côté, certaines entités mettaient l'accent sur les aspects stratégiques, notamment sur les effets que les atteintes à la cybersécurité pouvaient avoir sur la réputation, la productivité et les finances institutionnelles ; à l'autre extrême, certains registres portaient presque exclusivement sur la sécurité des systèmes informatiques et de communication, la préoccupation première étant de préserver la disponibilité de l'information, plutôt que sa confidentialité ou son intégrité. Dans ce second cas, les mesures requises sont plus complexes que celles qui visent seulement à éviter les perturbations techniques ou l'immobilisation, ce qui peut expliquer pourquoi elles figurent moins dans les documents examinés. Un des inconvénients des registres des risques centrés sur les aspects techniques de la cybersécurité est qu'ils pourraient ne pas faire le lien entre ces éléments et les répercussions plus larges pour l'entité.

Figure V
L'inclusion de la cybersécurité dans les registres des risques institutionnels, en nombre d'entités participantes



Source : Questionnaire du CCI (2020).

62. **La nécessité d'accorder une plus grande attention aux mesures d'atténuation.** Les données, même limitées, obtenues par les Inspecteurs ont mis en évidence la question de la formulation des mesures d'atténuation des cyberrisques, que ce soit dans le cadre de la gestion du risque ou en dehors de celui-ci. Comme souligné par les comités d'audit et de contrôle, les mesures d'atténuation sont souvent descriptives du statu quo (notamment lorsqu'elles détaillent des mesures déjà en place au lieu d'envisager, à titre préventif, des

tâches à entreprendre en prévision de risques spécifiques). Il en résulte un processus intéressé par lequel sont fixés des objectifs qui, ayant déjà été réalisés, vont améliorer les résultats communiqués, alors que des efforts sincères devraient être consacrés à la conception de véritables tâches d'atténuation constituant les jalons d'une mise en œuvre progressive. Sans perdre de vue que certaines entités peuvent avoir fait le choix délibéré de présenter leurs mesures d'atténuation en des termes assez généraux pour protéger leurs défenses, **les Inspecteurs sont d'avis qu'à l'avenir, l'accent devrait être mis sur la formulation de mesures d'atténuation, dans une optique prospective, qui tiennent compte des contraintes et faiblesses existantes, reconnaissant le fait que la réalisation de nouveaux objectifs peut nécessiter des efforts supplémentaires ainsi qu'une période de transition pendant laquelle les rapports pourraient avoir à rendre compte d'objectifs qui ne seraient pas pleinement réalisés.**

63. **Les feuilles de route.** Dans certains cas, l'évaluation des cyberrisques a conduit à l'adoption d'une feuille de route institutionnelle pour l'amélioration de la cyberrésilience de l'entité. Établie par la direction en prenant en compte les observations des parties prenantes internes, la feuille de route est, dans de nombreux cas, soumise à l'approbation des organes délibérants ou directeurs. Les Inspecteurs ont constaté que ces feuilles de route étaient au plus utiles lorsqu'elles prenaient la forme d'un plan pluriannuel assorti de jalons et d'indicateurs de réalisation, et s'accompagnaient d'une réorientation dans l'allocation des ressources pour que les mesures d'atténuation puissent être mises en œuvre dans la pratique. Au moment d'établir le présent rapport, des feuilles de route étaient ou avaient été mises au point dans plusieurs entités (l'OACI, l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO), le Fonds des Nations Unies pour la population (FNUAP), le Haut-Commissariat des Nations Unies pour les réfugiés (HCR), le Bureau des Nations Unies pour les services d'appui aux projets (UNOPS) et l'OMPI), et le fait de s'en pourvoir était considéré comme une bonne pratique pour rationaliser les efforts d'amélioration dans toute l'entité.

64. **Le passage de la prise de conscience à la gestion anticipative des risques.** En conclusion, bien que de nombreuses entités participantes aient compris l'importance des considérations de cybersécurité et tenté de les incorporer, à divers degrés de formulation, dans leurs cadres plus larges de gestion des risques, le tableau général, à l'échelle du système, reste inégal et nécessite qu'on y consacre l'attention voulue pour passer de la simple conscience des cyberrisques à leur gestion en bonne et due forme selon les besoins de chaque entité, tout en sachant que dans ce domaine, le risque zéro est irréalisable. **Par conséquent, les Inspecteurs souscrivent et font écho à la prudence prônée par les spécialistes de la cybersécurité : l'enjeu est de taille et une approche axée sur les risques s'impose (annexe II).** À l'avenir, l'accent doit être mis sur la mise au point de véritables mesures d'atténuation des risques qui devront s'accompagner d'une solide planification de la continuité des opérations. La contribution et la pleine participation des spécialistes de la cybersécurité aux processus internes de gestion des risques, depuis leur conception jusqu'à leur mise en œuvre et leur surveillance, sera cruciale pour réaliser ces objectifs.

C. Parti à tirer de la convergence entre sécurité physique et cybersécurité

65. **La démarcation est floue entre la sécurité physique et la cybersécurité.** La question quelque peu philosophique de savoir si la cybersécurité devait se concevoir principalement comme une matière relevant de la sphère « cyber », axée sur la technologie, ou de la sphère « sécurité », comparable à la sûreté et à la sécurité physiques, mais transposée au numérique, s'est posée très tôt dans le cadre du présent examen, même pendant sa conceptualisation, et a suscité un vif débat parmi les parties prenantes interrogées par les Inspecteurs. Bien que les entités des Nations Unies aient traditionnellement considéré séparément la sûreté et la sécurité physique, d'une part, et la cybersécurité, de l'autre, ce n'en sont pas moins des domaines qui concernent tous deux la protection du personnel et la préservation des avoirs. Dans ce but, les deux fonctions consistent à gérer l'incertitude ou le risque, c'est-à-dire à anticiper les attaques, à protéger contre elles et à savoir que faire lorsqu'elles surviennent, ce qui fait de la gestion du risque le dénominateur commun de ces deux domaines. La sécurité physique et la cybersécurité ont également en commun le constat

que même les meilleures mesures ne pourront garantir que les défenses d'une entité, quelque perfectionnées et solides qu'elles soient, ne seront pas percées par une attaque. Enfin, lorsqu'il a été question d'évoquer des situations montrant où finissait la cybersécurité et où commençait la sécurité physique, ou vice-versa, il est vite devenu évident que les sphères physiques et numériques n'étaient pas aussi distinctes qu'il n'y paraissait à première vue.

66. **La convergence entre la sécurité physique et la cybersécurité dans la pratique.** De nos jours, les systèmes d'appui à la sûreté et à la sécurité qui fonctionnent sans recourir, d'une façon ou d'une autre, aux TIC sont l'exception plutôt que la règle. C'est pourquoi lorsqu'une atteinte à la cybersécurité touche de tels systèmes, les conséquences se feront sans doute sentir dans le monde physique, parfois même au point d'exposer la vie ou l'intégrité physique de personnes à de grands dangers. Il ne manque pas d'exemples de situations pratiques dans lesquelles la cybersécurité et la sécurité physique se recoupent. Ainsi des hackers peuvent-ils prendre le contrôle d'une barrière de sécurité, exploiter les faiblesses d'un protocole de sûreté pour implanter un logiciel espion dans des appareils électroniques ou télécharger des renseignements personnels confidentiels sur des appareils portables, accéder en ligne aux plans d'étage de bureaux pour décider de la meilleure cible pour une attaque armée, ou se livrer à des vols d'identités virtuelles pour entraîner des utilisateurs dans des situations où ils vont finir par se mettre en danger à leur insu, en se fiant à des informations provenant de sources normalement fiables dont l'identité a été usurpée par des cybercriminels. Inversement, lorsque des mesures de sécurité poreuses compromettent la protection des locaux, des centres de données, des salles de serveurs ou des points d'accès numériques contre l'accès non autorisé ou d'autres interférences résultant de dangers physiques (naturels ou d'origine humaine), des répercussions directes peuvent se faire sentir dans la sphère numérique. La convergence des deux mondes peut apparaître plus évidente encore sur les présences hors siège, qui tendent à être plus éloignées des dispositifs centraux de contrôle et de surveillance de la cybersécurité, et peuvent aussi constituer des cibles plus attrayantes étant donné que l'information qui y est détenue touche directement à la vie et à l'intégrité physique, comme dans le cas des données relatives aux coordonnées ou déplacements du personnel dans des zones moins protégées.

67. **Le caractère encore sporadique des liens institutionnalisés entre sécurité physique et cybersécurité.** Les réponses faites aux questionnaires du CCI et les entretiens subséquents avec des responsables ont révélé que les entités avaient pris conscience à différents degrés des rapports qui existaient entre la sphère physique et la sphère numérique. Seules deux entités ont une architecture institutionnelle qui reflète l'intégration des cadres de gestion de la sûreté et de la sécurité physiques, d'une part, et de la cybersécurité, d'autre part, soit parce que les deux fonctions relèvent du même département et son rattachées hiérarchiquement à la même direction exécutive adjointe chargée de la sécurité au niveau de l'entité (OMPI), soit parce que, stratégiquement parlant, elles contribuent, comme de nombreuses autres, au « cadre de gestion de la résilience organisationnelle » qui, de façon plus large, combine les défenses contre tous types de menaces, qu'elles soient physiques, numériques, politiques, naturelles ou autres (UIT). D'autres entités, ayant reconnu qu'il y avait des points de convergence et des synergies à exploiter, ont officialisé dans une certaine mesure la coordination et l'échange d'informations entre les deux fonctions, au moyen, par exemple, de rapports hiérarchiques indiqués en pointillé, d'exposés conjoints à l'intention de l'équipe de direction ou de participation croisée aux réunions, ou encore en faisant en sorte que les deux fonctions contribuent sur un pied d'égalité aux processus institutionnels, comme la gestion du risque et la planification de la continuité des opérations, ou aux interventions en cas d'urgence nécessitant leur double participation à titre ponctuel. De même qu'existe déjà une collaboration dans le cadre de mesures spécifiques à caractère opérationnel (comme la mise en commun d'informations concernant les menaces à la cybersécurité et les menaces physiques dans le cadre des avis aux voyageurs en mission ou la conception conjointe de solutions technologiques sophistiquées pour l'identification et les cartes du personnel en vue de l'accès aux locaux), qui se traduit par certains avantages tangibles pour le dispositif de sécurité des entités concernées. Même dans des parties du système où la sûreté et la sécurité physiques sont considérées comme distinctes du cyberespace, sans grand rapport avec celui-ci, les entités ont donné des indications de contacts occasionnels et informels entre les deux fonctions. Il reste que, pour la majorité des entités qui ont répondu sur ce point, le lien entre la sécurité physique et la cybersécurité est sous-estimé ou reconnu de façon marginale, ce qui est également le cas au niveau du système dans son ensemble (par. 159 à 164).

68. **Relèvement des capacités en matière de cybersécurité au sein de la fonction de sûreté et de sécurité physiques.** De l'avis des Inspecteurs, il serait possible de tirer parti de la convergence entre la sécurité physique et la cybersécurité à l'avantage des deux domaines ainsi que de la résilience institutionnelle dans un sens plus large. Une possibilité consisterait à examiner la question du renforcement des capacités internes par le relèvement et l'élargissement du profil d'un nombre suffisant d'administrateurs de la sûreté et de la sécurité et d'incorporer des aspects de la cybersécurité dans leurs compétences à l'avenir, notamment en repensant la façon dont les définitions d'emploi sont formulées (par exemple, en y ajoutant des éléments de traitement des renseignements relatifs aux menaces à la cybersécurité, de modélisation des menaces et d'autres capacités analytiques du même ordre). La perception de la cybersécurité comme étant intrinsèquement sans rapport avec les fonctions de tels administrateurs et dissociée de celles-ci pourrait tenir à la pratique établie de longue date de recruter ce personnel principalement parmi les forces de police et les forces armées − une façon de voir les choses qui néglige le fait que ces dernières ont déjà développé leurs capacités dans les domaines concernés. Les compétences techniques existent, à charge pour les entités des Nations Unies de les recruter. Une fois acquises, ces capacités supplémentaires viendraient non pas remplacer, mais compléter l'appareil perfectionné et bien rodé que sont les effectifs actuels orientés vers la sécurité traditionnelle, et leur permettre d'interagir plus efficacement avec les capacités propres à la cybersécurité au sein des entités des Nations Unies concernées. Les Inspecteurs reconnaissent que les deux domaines se caractérisent par des capacités distinctes et hautement spécialisées, bien conçues pour servir leurs objectifs de protection respectifs, et qu'il serait par conséquent déraisonnable d'envisager de les fusionner en une seule structure ou d'en incorporer une dans l'autre sans un examen plus approfondi. Cela étant, la possibilité d'étoffer les capacités existantes pour améliorer les liens entre les deux domaines pourrait être une des voies à étudier dans la perspective d'une approche plus globale de la protection du personnel et des actifs des entités, comme envisagé dans la recommandation 5.

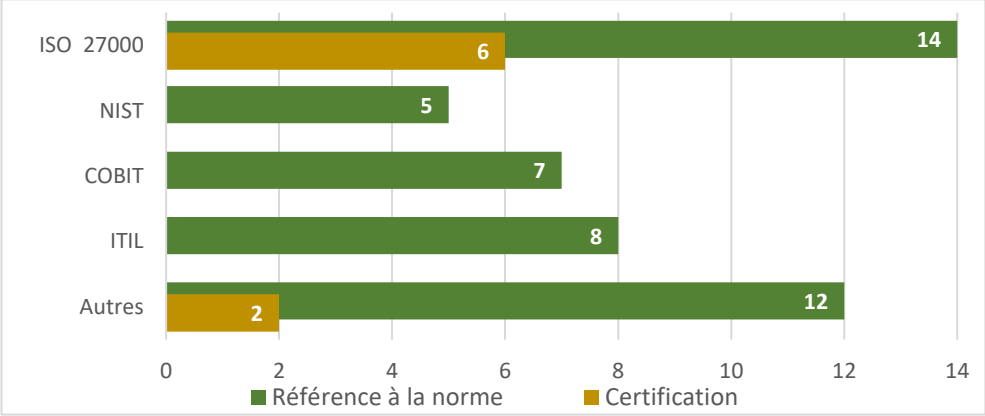
D. Élaboration de cadres réglementaires pour le respect des règles et la responsabilisation

Normes relatives à la sécurité de l'information

69. **Les normes utilisées par les entités participantes.** La cybersécurité est un domaine qui a fait l'objet d'un certain nombre de normes nationales et internationales qui fournissent des indications et des critères pour la mise en place de systèmes résilients de gestion de la sécurité informatique. L'expression « Management de la sécurité de l'information » retenue par l'Organisation internationale de normalisation (ISO) renvoie à la totalité des mesures qui, sur les plans de la gestion, de la réglementation et de la technologie, constituent le dispositif de cybersécurité d'une entité. Il s'agit d'un ensemble complexe de mesures allant notamment des règlements et des documents d'orientation aux outils et processus de gestion, concepts de sécurité et stratégies de gestion du risque. Les entités participantes ont mentionné un large éventail de ces normes, parfois plus d'une par entité, qu'elles ont dit avoir sélectionnées parce qu'elles correspondaient à leurs circonstances et exigences propres, puis affinées en consignant les mesures de référence les plus pertinentes dans une « déclaration d'applicabilité » spécialement conçue. Les Inspecteurs rappellent qu'il y a dix ans déjà, en 2011, le Réseau Technologies de l'information et des communications avait approuvé l'application de la norme ISO 27001 aux organismes des Nations Unies[16], et qu'en 2017, le Groupe d'intérêt pour la sécurité informatique avait réaffirmé cette position. Le présent examen confirme que la plupart des entités des Nations Unies ont obtenu la certification, envisagent de l'obtenir ou ont choisi de s'y conformer volontairement, sans chercher à officialiser la chose. Parallèlement à la norme ISO 27001, plusieurs autres normes sont utilisées par les entités des Nations Unies, comme indiqué dans la figure VI ci-dessous et détaillé dans l'annexe III. Seules trois entités n'ont signalé aucune référence à une norme ou n'ont pas communiqué d'information à ce sujet.

[16] CEB/2011/HLCM/ICT/16 (en anglais).

Figure VI
Principales normes externes utilisées par les entités participantes du CCI



Source : Questionnaire (2020) et entretiens du CCI.

Abréviations : NIST, National Institute of Standards and Technology (États-Unis) ; COBIT, Objectifs de contrôle de l'information et des technologies associées ; ITIL, Information Technology Infrastructure Library.

70. **Certification officielle contre référence aux normes.** En ce qui concerne l'utilité d'une certification officielle par rapport à des formes moins strictes de conformité volontaire, les Inspecteurs ont constaté que les avis des spécialistes divergeaient. C'est en effet une décision de gestion que de briguer une certification pour les assurances fiables qu'elle donne aux organes délibérants et directeurs, comme aux partenaires externes, par le caractère officiel de son processus et de la déclaration qui sanctionne celui-ci, ainsi que par la rigueur nécessaire aux vérifications annuelles indépendantes que nécessite son maintien. Elle peut également servir de déclencheur récurrent à l'innovation, par les améliorations constantes dont les systèmes doivent pouvoir faire état. Certaines entités font toutefois valoir que la certification peut s'avérer trop onéreuse et laborieuse pour être justifiable. Ils critiquent également le fait qu'elle repose dans une large mesure sur une conformité formelle, ce qui peut encourager la communication d'informations délibérément favorables au détriment de comptes rendus plus réalistes. Les Inspecteurs reconnaissent que les deux approches, à savoir la certification et l'alignement, peuvent s'avérer utiles, surtout à différents stades de le la mise en place graduelle de cyberdéfenses. C'est d'autant plus vrai que les normes peuvent être utilisées de différentes façons, notamment comme points de comparaison ou comme cadres à des fins de vérification, comme feuilles de route internes pour l'auto-amélioration, comme incitation supplémentaire à satisfaire aux contrôles de conformité, ou comme sources d'inspiration ou de référence pour la conception d'approches sur mesures.

71. **Les avantages de la référence aux normes.** Les Inspecteurs s'abstiennent de plaider en faveur de telle ou telle norme ou de l'adoption harmonisée, à l'échelle du système, de l'une ou l'autre d'entre elles, car différentes normes peuvent valablement servir différents objectifs et se présenter comme des choix opportuns selon le degré de maturité des systèmes. Il n'y a donc pas qu'une seule norme qui convienne, pas plus qu'il n'y a qu'une seule façon de concevoir la cybersécurité, mais il semble judicieux de s'inspirer − formellement ou informellement − des normes pertinentes pour la création et la gestion d'un cadre réglementaire propre. Il appartient donc aux entités participantes de sélectionner la norme qui leur convient et, dans le cadre de celle-ci, les mesures de référence les plus adéquates, compte tenu du degré de protection requis par leur situation et conformément aux exigences et aux risques relevés à l'issue d'une évaluation fiable et individualisée. Les Inspecteurs relèvent, sans poser de jugement, que la décision de l'entité à cet égard peut aussi avoir des implications au niveau du système dans son ensemble, l'utilisation du même cadre ou de la même norme pouvant faciliter les comparaisons et instaurer un langage commun à toutes ses composantes. La variété des approches peut, quant à elle, dans le contexte des mécanismes interentités, donner aux entités une occasion supplémentaire de débattre entre elles, de vérifier des hypothèses, d'examiner de façon plus critique leurs propres choix par rapport à ceux des autres, et d'apprendre les unes des autres de façon plus générale, autant de possibilités qui en définitive leur seront bénéfiques à titre individuel.

Cadres d'orientation et procédures

72. **La prérogative des entités de se doter de leur propre cadre réglementaire.** Il n'y a pas, en dehors des diverses normes susmentionnées, de consignes universellement et directement applicables qui fassent autorité quant à la réglementation des questions de cybersécurité. L'absence d'instrument ou de cadre juridique international à cet égard peut être attribuée au fait que le domaine lui-même comporte de multiples facettes et est difficile à délimiter, de sorte que sa réglementation est une entreprise complexe même au niveau de la législation d'un seul État. Porter cette complexité au niveau international rend encore plus ardue la définition d'un cadre commun régissant les relations entre les parties prenantes, que ce soient les États ou les autres acteurs du cyberespace, relevant des secteurs public ou privé. À ce stade, il n'y a ni instrument contraignant au regard du droit international, ni le moindre cadre normatif applicable aux Nations Unies qui réglemente spécifiquement la cybersécurité. Il s'ensuit que la meilleure description du cadre international de gouvernance du cyberespace est celle d'un patchwork d'institutions et de normes formelles et informelles où s'entrecoupent et se superposent normes techniques, contrats, lois et décisions intergouvernementales. Faute d'un cadre cohérent qui puisse servir de modèle, chaque entité conserve la prérogative − dans les limites des paramètres que dictent son instrument fondateur et les décisions connexes de ses organes délibérants et directeurs − de formuler ses propres règles de façon relativement autonome et d'arrêter le schéma selon lequel s'organisera sa cybersécurité.

73. **La référence habituelle faite à la cybersécurité dans les stratégies relatives aux TIC.** La façon dont la cybersécurité est traitée dans les cadres réglementaires existants, c'est-à-dire dans l'environnement normatif où s'exercent les fonctions institutionnelles, varie d'une entité à l'autre et tend à refléter l'évolution historique de la cybersécurité en tant que matière issue de la sphère des TIC et devenue, à force de croître, une discipline à part entière. De rares organisations la conçoivent tout à fait indépendamment des TIC, la considérant comme une matière à part entière sur un pied d'égalité avec la sécurité physique (OMPI) ou en tant que composante du domaine plus large de la gestion de la résilience (UIT). Ces démarches restent toutefois exceptionnelles, la plupart des entités ayant élaboré un document stratégique pluriannuel qui expose leur projet pour les TIC en incorporant des dispositions relatives à la cybersécurité. Dans certains cas, il ne s'agit toutefois que d'une référence élémentaire, parfois complétée par des orientations plus détaillées à un niveau stratégique inférieur, tandis que dans d'autres, le sujet se voit consacrer des chapitres entiers. **Indépendamment de la mesure dans laquelle les consignes de cybersécurité sont développées dans les stratégies relatives aux TIC des entités, les Inspecteurs estiment que les références à la cybersécurité dans ce cadre stratégique sont un premier pas positif.**

74. **L'existence ou l'élaboration de politiques de cybersécurité au sein de nombreuses entités participantes.** Il importe de noter que les textes de base de plusieurs grandes normes considèrent l'existence de politiques et de procédures avérées en matière de cybersécurité comme une des composantes essentielles des mesures de contrôle qui sont à la base d'un système de gestion de la sécurité de l'information[17]. Le présent examen a permis de constater que de nombreuses entités avaient produit de telles orientations spécifiques, et qu'à quelques exceptions près, celles qui ne l'avaient pas fait étaient en train d'en élaborer. Pour être plus précis, selon les informations reçues, 17 entités avaient mis en place des instruments de réglementation spécifiquement consacrés à la cybersécurité (dont trois sont en cours de révision), tandis que quatre ont confirmé qu'elles étaient en train de mettre au point de nouvelles politiques. Seules trois entités ont indiqué ne pas avoir formulé ou ne pas être en train de formuler de politiques ou de réglementations spécifiques à la cybersécurité, déclarant

[17] La norme ISO 27001 ouvre sa liste normative d'objectifs et de mesures de référence par le titre « A.5 Politiques de sécurité de l'information ». Elle y prescrit notamment comme mesure la définition d'un ensemble de politiques de sécurité de l'information et sa communication aux salariés et aux tiers concernés. Dans son document de base intitulé « *Framework for Improving Critical Infrastructure Cybersecurity* » (cadre pour l'amélioration de l'infrastructure critique de cybersécurité), sous la catégorie consacrée à la gouvernance, le National Institute of Standards and Technology (États-Unis) précise que « les politiques, procédures et processus » servent à informer « le management des risques en matière cybersécurité ».

qu'elles s'appuyaient sur leurs politiques et procédures relatives aux TIC à cet égard. Il est donc permis de dire qu'à de rares exceptions près, les entités ont reconnu qu'il était important de disposer d'un cadre de référence clairement défini pour orienter leur démarche de cybersécurité. L'annexe IV énumère les principaux instruments régissant la cybersécurité dans les cadres réglementaires des entités participantes.

75. **Cadres généralement complexes, hétérogènes et à plusieurs niveaux.** Les cadres réglementaires constatés par les Inspecteurs, indépendamment du fait que certaines entités en aient adopté de plus élaborés ou que d'autres se réfèrent à ceux qu'elles avaient établis pour les TIC plus généralement, tendaient à être dispersés parmi un ensemble de documents de stratégie, d'orientation générale, de procédure et d'encadrement technique. La terminologie associée à ces documents variait selon les entités participantes, allant de la stratégie à l'exposé de mission, de la politique à l'instruction administrative, des instructions permanentes aux lignes directrices, et du guide au protocole, ces notions se recouvrant souvent, même au point d'être interchangeables. Le CIC a réalisé un modèle pour représenter les différentes composantes normatives du système de gestion de la sécurité de l'information sous forme de couches, le niveau d'abstraction le plus élevé étant au sommet et le niveau le plus détaillé à la base. Il a aidé plusieurs entités des Nations Unies à évaluer et à améliorer leurs cadres de réglementation et de gouvernance existants. À partir de ce modèle, l'annexe IV présente une vue d'ensemble des objectifs, formats et contenus typiques que les Inspecteurs ont relevés dans les documents institutionnels relatifs à la cybersécurité et aux TIC qu'ils ont examinés, reconnaissant qu'une analyse qualitative détaillée des contenus dépasserait le cadre du présent examen.

76. **L'adaptation au contexte et l'examen périodique.** Pour veiller à ce que ses politiques correspondent à ses spécificités, une entité peut avoir à ajuster les premières pour refléter plus exactement les mesures de référence préconisées par les normes externes auxquelles elle a choisi, le cas échéant, de se conformer. Des exemples de cette façon de procéder ont été relevés au PAM et au PNUD, où, pour chaque mesure technique de la norme ISO 27001 sélectionnée aux fins de sa « déclaration d'applicabilité », l'entité avait fait figurer une déclaration de politique générale dans son cadre réglementaire. Il peut aussi s'agir de réglementer des domaines présentant un intérêt plus particulier pour certaines entités que pour d'autres. C'est notamment le cas des orientations relatives aux pratiques sûres applicables à la création de sites Web, de bases de données ou d'applications propres. La variété des politiques et les différentes configurations des cadres réglementaires étudiés peuvent donc valablement s'expliquer, du moins en partie, par la nécessité de les adapter à la réalité de l'entité, plutôt que par un manque de systématisme dans la réglementation. En outre, dans un domaine qui connaît une évolution aussi rapide que celui de la cybersécurité, il est d'autant plus important que les orientations normatives restent suffisamment adaptables et pertinentes, ce que certaines entités ont recherché en soumettant leurs orientations à des examens périodiques. À cet égard, il peut être considéré de bonne pratique d'inclure dans les documents d'orientation et dans les politiques des échéances explicites auxquelles elles doivent être officiellement examinées et, si nécessaire, révisées, non sans mentionner à qui revient la responsabilité d'engager ces processus.

77. **L'importance de l'existence de consignes, quels que soient leur portée, degré de détail ou contexte institutionnel.** Étant donné la grande variété des questions relatives à la cybersécurité susceptibles d'être réglementées, il est difficile de relever, et encore plus de prescrire, les types précis de règles ou de procédures qui serviraient au mieux un solide cadre de cybersécurité. On se bornera à dire que l'existence d'orientations même élémentaires dans ce domaine aux aspects hautement techniques et aux multiples facettes est importante pour une application cohérente et homogène des mesures de sécurité, indépendamment de la taille de l'entité ou des ressources à sa disposition.

Intégration de la cybersécurité

78. **L'intégration.** Ce serait faire preuve d'une vision étroite de la réalité que de s'arrêter aux politiques relatives aux TIC et à la cybersécurité dans l'élaboration d'un cadre réglementaire à l'appui d'une plus grande résilience institutionnelle. Les cyberdéfenses d'une entité sont une responsabilité que se partagent de nombreux services. L'intégration peut s'avérer d'une grande utilité pour l'adoption d'une démarche à l'échelle de l'entité qui soit

organique plutôt qu'imposée (par. 92 à 95). Un certain nombre d'entités ont d'ores et déjà entrepris d'intégrer la cybersécurité dans leurs différentes politiques. Il faudrait toutefois une analyse d'une portée beaucoup plus large et une étude plus approfondie que celles que permet le présent examen pour évaluer la mesure dans laquelle la cybersécurité a été intégrée dans les cadres réglementaires globaux des entités participantes. Dans l'encadré 4, les Inspecteurs fournissent quelques indications qui peuvent être prises en compte à cet égard.

Encadré 4
Indications pour l'intégration de la cybersécurité dans les cadres réglementaires institutionnels

- Des éléments relatifs à la cybersécurité peuvent être incorporés directement dans les politiques, processus et pratiques qui orientent le travail de services tels que les ressources humaines, les achats, les communications ou les affaires juridiques. Par exemple, une procédure d'agrément spécifique conditionnant l'engagement de fournisseurs de services peut être incluse dans le manuel des achats, et les étapes à suivre pour gérer les cyberrisques tout au long du cycle de vie des projets peuvent être incluses dans le modèle du descriptif de projet ou dans les documents programmatiques destinés à servir de guides aux unités administratives dans leurs activités quotidiennes.
- Les rôles et responsabilités de services ou fonctions autres que ceux qui s'occupent directement des TIC ou de la cybersécurité peuvent être attribués et expressément visés dans les principaux instruments de réglementation en vigueur. Par exemple, la politique institutionnelle de sécurité des technologies de l'information du PAM précise les rôles et responsabilités de différentes catégories de personnes telles que les propriétaires et dépositaires de l'information, les superviseurs et le personnel. L'OMPI est un autre exemple.
- Des dispositions peuvent être prises pour que toutes les parties prenantes au-delà du personnel des services chargés des TIC et de la cybersécurité soient appelées à contribuer de façon régulière non seulement à la formulation de ces instruments, mais aussi à leur application (par exemple, en permettant à des représentants de ces parties prenantes de siéger au sein des organes de gouvernance concernés ou en prévoyant un processus d'approbation des politiques selon lequel certaines parties prenantes doivent être consultées avant que ne soit arrêté le texte final).

Source : Établi par le CCI.

Respect des règles et responsabilisation

79. **L'accessibilité des règles en tant que préalable à leur respect.** L'efficacité d'un cadre réglementaire, aussi bien formulé soit-il, sera toujours tributaire de la mesure dans laquelle les parties concernées se conformeront aux règles. Le respect des directives peut être influencé par plusieurs facteurs, y compris l'accessibilité de textes qui exposent en termes clairs ce qui est attendu de chaque partie prenante et de chaque membre du personnel, et le pourquoi de ces exigences. Un responsable de la sécurité de l'information a mis ce dernier point en exergue lors de son entretien avec les Inspecteurs, faisant observer que le problème n'était pas tant le manque de consignes écrites que le manque de compréhension, chez les utilisateurs, de la raison pour laquelle les règles existaient, de ce qu'elles protégeaient et des effets que leur méconnaissance pouvait avoir sur l'individu et l'entité. L'importance de cette prise de conscience fait l'objet de développements ailleurs dans le présent rapport (par. 97 à 103). Elle doit notamment s'opérer par l'utilisation, à l'intention des utilisateurs, d'un mode d'expression et de messages simples, non techniques et avenants qui s'efforcent de rendre palpables les conséquences que peut avoir un comportement risqué en ligne. Un exemple de centre documentaire bien structuré consacré à la cybersécurité est fourni par le Secrétariat de l'ONU. Il suffit d'un clic sur la page Intranet du Bureau de l'informatique et des communications pour obtenir des vidéos en langue simple, des affiches, des miniguides, des réponses aux questions courantes, et la série complète des règlements et politiques, classés par sujet et assortis de notes explicatives.

80. **L'insuffisance possible de la démarche actuelle face au non-respect des règles.** Un facteur important et qui peut facilement jouer en faveur du respect des règles est l'existence de mesures de sanction efficaces en cas de non-respect, renforcées, idéalement, par le fait connu et prévisible qu'un comportement indu donnera effectivement lieu à sanction. Peu de politiques examinées par les Inspecteurs contenaient des dispositions visant spécifiquement la sanction d'entorses à la cybersécurité. Même lorsque des mesures spécifiques étaient mentionnées dans les politiques concernées, les informations recueillies concernant leur application dans la pratique donnaient à conclure qu'elles n'étaient guère imposées et que, par conséquent, les employés qui se livraient à des pratiques risquées n'avaient généralement pas à répondre de leurs actes. Dans la plupart des entités participantes, c'est la politique régissant l'usage correct des TIC qui, le cas échéant, comporte des dispositions spécifiques relatives aux sanctions pour usage abusif de ces technologies, ce qui recouvre généralement les atteintes à la cybersécurité. En général, ces violations sont passibles du même type de mesures disciplinaires que toute violation du règlement. Il reste que la procédure normale, même engagée et menée à terme sans encombre, est notoirement lente, lourde et onéreuse en ressources, et qu'elle tend à n'être ouverte que pour des cas d'inconduite particulièrement flagrants dans le domaine des TIC.

81. **La nécessité d'envisager un système de sanctions plus nuancées.** En ce qui concerne les entorses à la cybersécurité, qui souvent ne sont dues qu'à l'ignorance ou à l'imprudence, **les Inspecteurs sont d'avis que des sanctions plus aisées à mettre en œuvre, moins formelles et moins invasives pourraient constituer une approche plus prometteuse.** De telles sanctions permettraient en effet de traiter le problème d'une façon plus directe et immédiate, et proportionnelle à la gravité du comportement. Il convient toutefois de trouver un certain équilibre pour que les conséquences du comportement irrégulier soient suffisamment ressenties par la partie qui en est responsable, afin d'encourager une meilleure hygiène informatique et un comportement plus responsable. La reconnaissance implicite de cette logique peut être détectée dans la pratique de certaines entités qui font la distinction entre des entorses mineures et des manquements plus graves à leurs politiques de cybersécurité. Il n'est toutefois pas apparu avec la même évidence que ces entités étaient parvenues à traduire cette distinction en sanctions qui soient mieux adaptées aux faits mineurs tout en restant efficaces. Certaines politiques, par exemple, prévoient d'informer la hiérarchie ou le chef du service des TIC en cas de manquement. Cette mesure, qui pourrait constituer la seule pression « douce » disponible pour assurer le respect des règles, ne laisse cependant entrevoir aucune conséquence autre qu'un éventuel embarras. Un contre-exemple qui mérite d'être noté, en raison de sa spécificité et de ses effets indésirables sur l'utilisateur, sans avoir un caractère excessivement punitif pour autant, est fourni par l'AIEA, qui prévoit dans ses règles une sanction explicite, non disciplinaire, consistant à révoquer le droit de l'individu pris en défaut d'accéder aux systèmes informatiques. Il est également intéressant de noter que cette règle reconnaît la valeur de la proportionnalité, en ce qu'elle dispose que l'individu concerné doit avoir eu conscience de l'irrégularité de ses actes pour être sanctionné, et qu'elle met en équilibre l'objectif de protéger efficacement les actifs institutionnels et le souci d'éviter que l'application de mesures coercitives ne revienne à exercer des pouvoirs de police sur le personnel. En pratique, la révocation est imposée à titre temporaire et après des avertissements répétés. Les Inspecteurs souhaiteraient insister sur le fait qu'aucun régime de sanction digne de ce nom ne saurait être mis en œuvre sans l'assentiment explicite du chef de secrétariat, facteur qui a d'ailleurs contribué au succès de l'exemple cité. **De l'avis des Inspecteurs, les chefs de secrétariat devraient également étudier la possibilité d'introduire des incitations au signalement des incidents et d'encourager les individus à assumer la responsabilité de leurs pratiques dangereuses ou risquées.** Pour ce faire, il importera de trouver des moyens de concilier l'objectif de dissuasion au moyen de sanctions plus nuancées, et celui d'incitation à la communication sans crainte de répercussions.

E. Mise à profit des contributions des mécanismes de contrôle

82. **L'attention accordée à la cybersécurité à tous les niveaux d'audit et de contrôle.** Les Inspecteurs se sont penchés sur la façon dont les mécanismes de contrôle s'étaient intéressés aux questions de cybersécurité compte tenu de leurs compétences particulières, que ce soit au niveau de la fonction d'audit interne (portant avant tout sur le respect des règles

et des procédures), au niveau des audits externes (portant avant tout sur les comptes et la conformité, et occasionnellement sur des aspects de l'administration et de l'encadrement) ou au niveau des comités d'audit et de contrôle (chargés avant tout de conseiller sur des questions institutionnelles plus larges qui appellent une attention et des interventions prioritaires de la part des équipes de direction et des organes délibérants et directeurs). Les Inspecteurs saluent le fait qu'à chacun de ces niveaux, la cybersécurité figure parmi les questions d'intérêt depuis cinq ans, voire depuis plus longtemps dans certaines entités.

Organes de contrôle saisis de questions relatives à la cybersécurité

83. **Les audits internes et externes sont axés principalement sur les TIC, y compris sur la cybersécurité dans une certaine mesure.** Les questions relatives aux TIC sont généralement bien intégrées dans la planification des audits internes axés sur la gestion des risques. Les recherches du CCI n'ont cependant révélé qu'un nombre limité de tâches d'audit portant spécifiquement sur la cybersécurité au cours des cinq dernières années. En ce qui concerne les capacités de mener de telles tâches, seules quelques entités disposent de leurs propres spécialistes de l'audit informatique, la majorité faisant appel à des spécialistes externes. Cette façon de procéder semble satisfaisante dans la plupart des cas. Dans de nombreuses entités participantes, les TIC figuraient également parmi les domaines auxquels se sont intéressés les auditeurs externes au fil des ans, notamment sous l'angle de la continuité des opérations, de l'évaluation et de la gestion des risques, des politiques relatives aux TIC et de la gestion des actifs relatifs aux TIC. Dans l'ensemble, les réponses données par les équipes de direction aux Inspecteurs donnaient à conclure que les recommandations résultantes avaient été acceptées, indiquant les mesures qui avaient été prises pour les mettre en œuvre.

84. **L'attention soutenue accordée à la cybersécurité par les comités d'audit et de contrôle.** En 2016, les représentants des comités de contrôle de 19 entités des Nations Unies « ont notamment estimé que la gestion des risques liés à la cybersécurité dans un environnement numérique était une priorité et sont convenus de demander à l'Administration des comptes sur ses connaissances et son état de préparation dans ce domaine »[18]. De fait, à l'analyse des rapports de ces comités, il apparaît que le renforcement de la gouvernance et de la gestion des risques dans le domaine de la cybersécurité avait fait l'objet d'un intérêt soutenu, même s'il n'était spécifiquement question de cybersécurité dans aucun des mandats correspondants et que seuls quatre rapports faisaient référence aux TIC. Les comités se sont principalement penchés sur ces questions dans le cadre de leur mandat relatif à la gestion du risque institutionnel ou, le cas échéant, lorsqu'ils vérifiaient l'état de mise en œuvre de recommandations relatives aux TIC issues d'audits internes ou externes. Le présent examen a établi que les connaissances spécialisées en la matière n'étaient pas systématiquement présentes parmi les membres des comités d'audit et de contrôle, seuls quatre comités en ayant apparemment eu le bénéfice. La plupart faisaient appel à des conseils externes, selon les besoins, à l'instar des arrangements en vigueur au sein de la fonction d'audit interne. Il est louable que ces comités se soient saisis de la question, non seulement parce qu'ils peuvent ainsi aider les équipes de direction à faire leur une approche de la cybersécurité fondée sur la gestion des risques, mais aussi parce que c'est une façon d'informer les organes délibérants et directeurs des risques touchant à la cybersécurité, et de leur donner les moyens, partant, de contribuer à les atténuer.

Utilité des recommandations de contrôle pour améliorer le dispositif de cybersécurité des entités

85. **Les recommandations de contrôle, moteurs de changements structurels positifs.** Les entités participantes ont indiqué que leur approche de la cybersécurité avait connu d'importants changements structurels motivés par les recommandations issues des organes de contrôle, mettant ainsi en évidence la valeur ajoutée de ces mécanismes. Au cours des entretiens, les responsables des TIC et de la cybersécurité ont généralement dit apprécier les rapports de contrôle en tant que moteurs de changement et qu'outils de sensibilisation des équipes de direction à la nécessité de mettre davantage l'accent sur la constitution d'un

[18] Voir A/72/295, par. 40 à 43.

robuste dispositif de cybersécurité. Les Inspecteurs ont effectivement constaté des cas où des recommandations de contrôle interne avaient contribué de façon directe à l'amélioration de la cybersécurité au sein de l'entité concernée, notamment à l'OMPI. D'autres cas ont été relevés, à l'OACI et au FNUAP, où une recommandation de contrôle à conduit à l'élaboration d'une feuille de route pluriannuelle ; à l'UNESCO, où a été créé un poste de responsable de la sécurité de l'information ; ou encore au Secrétariat de l'ONU, où la participation à la formation sur la sécurité de l'information s'est sensiblement améliorée. Des auditeurs externes ont également formulé des recommandations concernant des questions touchant à la cybersécurité à l'intention de 16 entités participantes au cours des cinq dernières années, notamment en ce qui concerne la le taux de participation à la formation relative à la sécurité de l'information, la récupération de données, le contrôle de l'accès des utilisateurs et les ressources à consacrer à la cybersécurité. L'utilité des recommandations de contrôle semblait davantage reconnue lorsque, dépassant les questions de conformité, elles touchaient aux aspects opérationnels et techniques de l'entité et proposaient des améliorations stratégiques, la seule conformité aux cadres réglementaires n'étant pas une garantie de protection. Par ailleurs, de nombreuses entités se sont déclarées préoccupées par le fait que certaines des recommandations n'avaient pas pris suffisamment en compte les contraintes liées aux ressources et les réalités opérationnelles, ce qui réduisait les chances de mise en œuvre.

86. **La nécessité d'une fonction d'audit interne systématiquement éclairée par des connaissances spécialisées en cybersécurité.** Pour maximiser leur apport dans le domaine de la cybersécurité, il est important que les organes de contrôle disposent de toute l'information utile concernant les risques, les capacités et les contraintes relatives à ce domaine au sein d'une entité et qu'ils en aient une bonne compréhension. Le moyen le plus efficace d'arriver à cette fin est de veiller à ce que les informations et les connaissances dont disposent les spécialistes au sein de l'entité puissent éclairer et alimenter le travail de la fonction de contrôle. Diverses possibilités existent à cet égard, dont certaines ont déjà trouvé leur place dans la pratique ou même dans les cadres réglementaires des entités participantes, soit individuellement, soit de façon combinée. Elles peuvent être considérées comme de bonnes pratiques et comprennent les mesures suivantes : a) le responsable de la sécurité de l'information, ou le service concerné, est obligatoirement consulté pour planifier tout audit axé sur la gestion des risques, et il participe pleinement à la définition des mesures de référence et indicateurs concernés ; b) les informations concernant la cybersécurité sont fournies aux organes de contrôle selon les besoins de leurs mandats respectifs, que ce soit par la communication des indicateurs d'incidents, par des réunions d'information spéciales ou régulières, ou par d'autres moyens ; c) avant sa finalisation, tout rapport d'audit ou toute recommandation touchant à la cybersécurité est soumis au responsable de la sécurité de l'information, ou au service concerné, pour observations, afin de prévenir les préoccupations que suscitent les recommandations qui, faute d'être en phase avec les réalités institutionnelles, risquent de devenir inapplicables.

F. Établissement d'une culture de la cybersécurité : du sommet à la base

87. **La direction doit encourager la reconnaissance des erreurs et des vulnérabilités.** Comme examiné ci-dessus, le dispositif de cybersécurité d'une entité doit aussi pouvoir s'appuyer sur une forte culture interne. Celle-ci commence par l'attention et le degré de priorité accordés à la question par l'équipe de direction − le ton est donné au sommet. Elle ne doit pas en rester là, toutefois, et doit pouvoir être assimilée par chaque membre du personnel, sans exception. Il faut pour cela un engagement et une participation des échelons supérieurs de l'entité qui soient continus et qui dépassent de simples déclarations clamant le caractère prioritaire de la cybersécurité au sein de l'entité. À cet égard, un élément clé consisterait à encourager une culture interne dans laquelle le fait de reconnaître un incident ne serait pas vécu comme un échec, mais comme un point de départ pour résoudre un problème partagé et mieux protéger l'entité et ses actifs, les erreurs et les faiblesses étant le fait et la responsabilité de tout un chacun, collectivement et individuellement. La culture de l'application des lois telle qu'elle s'applique au domaine de la sûreté et de la sécurité humaines peut servir d'enseignement sur ce point : la survenue d'incidents est chose acquise, tout comme le fait que ceux-ci seront automatiquement déclarés et traités, sans jugement. **Les Inspecteurs considèrent qu'il incombe au chef de secrétariat d'implanter une telle culture dans**

toutes les fonctions de l'entité et dans tous les lieux où elle est présente, dès lors que les systèmes informatiques sont interconnectés et interdépendants, et qu'une attaque ou une intrusion en un point peut conduire à une atteinte en tous points.

88. **La prise de conscience et la responsabilisation de la direction exécutive comme point de départ.** Le premier pas vers l'assimilation d'un nouvel état d'esprit, d'une nouvelle culture, est franchi lorsque l'équipe de direction elle-même s'intéresse davantage à la question et prend conscience des risques associés à la cybersécurité ainsi que des conséquences que peuvent avoir l'inaction et la pratique d'une hygiène informatique douteuse. Pour ce faire, la direction peut demander à ce que des points réguliers lui soient faits par le personnel concerné, qui peut comprendre des spécialistes de la cybersécurité, des fonctionnaires de la gestion des risques et des représentants d'organes de contrôle, et à ce que des formations et des initiatives de sensibilisation soient mises sur pied à son intention. Depuis 2020, les contrats de mission des hauts fonctionnaires du Secrétariat de l'ONU, qui sont conclus entre le Secrétaire général et les intéressés, contiennent des dispositions conçues pour promouvoir la prise de conscience et la responsabilisation dans le domaine de cybersécurité. La cohérence et l'efficacité des contrats de mission et des indicateurs de performance qu'ils contiennent dépassent le cadre du présent examen, mais l'inclusion même d'objectifs de cybersécurité dans l'évaluation et la notation des hauts fonctionnaires est un pas encourageant qui tend à favoriser la responsabilisation et à donner le ton voulu au sommet de hiérarchie. Il convient en outre d'encourager, y compris au sein des entités elles-mêmes, des initiatives telles que l'exposé qui a été présenté dans le cadre du Comité de haut niveau sur la gestion pour appeler l'attention des équipes de direction sur les retombées continues des cyberrisques sur les opérations, qui se traduisent non seulement par la perturbation des systèmes, réseaux et infrastructures administratifs, mais aussi par la mise en péril de l'exécution des mandats de fond[19].

89. **L'argent seul ne suffit pas à acquérir une culture de la cybersécurité.** Il est de nombreux moyens concrets par lesquels les directions exécutives peuvent susciter l'action et influencer les mentalités en aval de la chaîne de commandement. L'allocation de ressources suffisantes est certes une façon de marquer l'importance accordée à la cybersécurité, mais l'argent seul ne saurait résoudre la problématique de l'état de préparation dans ce domaine, ni acheter une culture de la cybersécurité. Autrement dit, le fait de fournir un appui financier ne libère pas les directions exécutives de la responsabilité de se montrer investies dans les questions de cybersécurité, comme affirmé dans un récent rapport de Gartner, groupe de réflexion bien connu qui se consacre à la cybersécurité[20]. Un appui qui ne se manifeste que financièrement peut en fait déplacer la responsabilité sur l'échelon directement inférieur de la hiérarchie, où les fonds peuvent être utilisés sans le bénéfice d'un projet stratégique global. L'affectation des ressources et les investissements connexes doivent être décidés dans un contexte opérationnel plutôt que d'un point de vue purement technologique ou axé sur la gestion du risque, et la direction exécutive est la mieux placée pour prendre une décision éclairée à cet égard, en faisant la juste part des choses (par. 108 et 109).

90. **Les manifestations non monétaires de l'appui de la direction exécutive.** Les faits suivants font partie des bonnes pratiques auxquelles les chefs de secrétariat d'entités participantes ont eu recours pour manifester un appui non monétaire significatif à la culture de la cybersécurité : participer de façon visible à des programmes de sensibilisation, comme l'enregistrement vidéo de déclarations de soutien ; parler au personnel de questions de cybersécurité lors de réunions générales ; s'entretenir avec le personnel de cyberattaques personnellement vécues ; donner publiquement l'exemple de comportements recommandés ; appuyer des campagnes d'hameçonnage simulé destinées à tous les niveaux de personnel, y compris l'équipe de direction ; veiller à ce que les responsabilités fassent leur chemin du haut en bas de la hiérarchie et faire pression à cette fin sur les cadres supérieurs pour qu'eux-mêmes suivent des formations et investissent leurs équipes de la responsabilité de se conformer aux politiques et aux comportements recommandés ; soutenir l'imposition de sanctions proportionnées, en particulier lorsque sont visés des récidivistes qui violent continuellement les règles et les procédures de cybersécurité. Comme indiqué plus haut, le

[19] Voir CEB/2017/HLCM/ICT/9 (en anglais).

[20] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, février 2020.

point de départ consiste à reconnaître les faits lorsqu'une erreur a été commise, à en tirer les enseignements et à chercher ensemble, en tant qu'entité, à en résoudre les conséquences.

91. **Il faut du temps, des messages cohérents et l'engagement de la hiérarchie pour faire évoluer les mentalités.** Pour s'implanter dans les attitudes du personnel à tous les niveaux et donner forme, ce faisant, à une culture institutionnelle de la cybersécurité, les mesures préconisées devront être réitérées, et elles mettront du temps à produire des résultats. L'expérience montre que les chances de réussite seront à la fois accrues et accélérées lorsqu'un message cohérent, insistant sur l'importance et la permanence de l'effort de cybersécurité, vient du sommet de l'entité. Comme il a été dit au huitième symposium du Groupe d'intérêt pour la sécurité informatique en 2019, changer le comportement humain est une tâche ardue qui s'accomplit par l'exposition répétée et cohérente à des messages porteurs d'informations nouvelles, par un réapprentissage périodique et par la compréhension des risques latents associés à la technologie ainsi que des conséquences des mauvais comportements informatiques[21].

G. Adoption d'une démarche à l'échelle de l'entité

92. **Le rôle des unités administratives.** La réalisation croissante du fait que la cybersécurité ne pouvait être l'affaire des seuls services des TIC a amené la majorité des entités participantes à reconnaître, d'une façon ou d'une autre, que les unités administratives comme organiques avaient un rôle à jouer dans ce domaine. Il ressort des réponses aux questionnaires du CCI que cette réalisation pourrait être plus prononcée dans les unités administratives. En fait, que cela soit formellement inscrit ou non dans les cadres réglementaires de leurs entités, plusieurs unités administratives ont déjà pour habitude de contribuer à la maintenance des protections de cybersécurité au niveau institutionnel. Ces contributions peuvent prendre les formes suivantes : le service des ressources humaines qui facilite un programme de formation à la cybersécurité ; le service des achats qui s'occupe des relations avec un fournisseur de services externes, notamment de son agrément en matière de cybersécurité ; le service juridique qui conseille sur des questions de réglementation, de contrats ou de conformité ; le service chargé de la communication qui gère les relations publiques avec les parties prenantes externes. Outre ces contributions relevant de leurs fonctions, la plupart de ces services devraient être naturellement disposés à incorporer la cybersécurité dans leurs activités quotidiennes, étant donné que le traitement d'informations sensibles, notamment personnelles et financières, est au cœur de leur travail. Les documents étudiés par le CCI ne permettent pas de dire si cette incorporation a atteint un degré suffisant et si elle signifie que ces services ont bien compris leur rôle privilégié en tant que dépositaires d'informations sensibles. Cet aspect des choses mérite peut-être que les chefs des services concernés et les auditeurs internes s'y intéressent de plus près, de même qu'il pourrait figurer, le cas échéant, dans les évaluations de la cybersécurité établies par des fournisseurs externes.

93. **Le rôle des unités organiques.** Les informations recueillies pour réaliser le présent examen donnent à penser que, contrairement aux unités administratives, et à l'exception des entités participantes dont les mandats accordent une place centrale à la stricte confidentialité des données, la cybersécurité est souvent considérée comme une charge administrative et une contrainte opérationnelle par les responsables des unités organiques. Si l'on en croit les informations reçues, les bureaux de programme n'étaient pas assez ouverts à la nécessité d'inclure des critères de cybersécurité et de résilience dans la conception et l'exécution de leurs projets et activités. Aux dires d'un responsable de la sécurité de l'information interrogé, les règles et procédures de cybersécurité sont souvent considérées comme un obstacle à la rapidité d'exécution plutôt que comme un bouclier pour protéger la réputation et les actifs des entités ainsi que le bon déroulement de leurs opérations. Sur cette toile de fond, il est particulièrement important que les chefs de secrétariat s'emploient activement à combattre l'idée selon laquelle le renforcement des mesures de cybersécurité fait obstacle à la souplesse des opérations ou à la réalisation des objectifs visés par les mandats.

[21] CEB/2019/HLCM/DTN/02 (en anglais).

94. **L'intégration et l'appropriation des rôles et des responsabilités sont les clés d'une approche à l'échelle de l'entité.** Comme indiqué ci-dessus (par. 78), le fait d'intégrer des considérations de cybersécurité dans les règles qui président aux activités de chaque service reviendrait à reconnaître que chaque fonction doit contribuer à l'approche globale de son entité. Au vu de la tendance récente de nombreuses entités à décentraliser et à déléguer l'autorité au niveau des cadres moyens, l'intégration favoriserait aussi une appropriation et une responsabilisation plus directe dans toute l'entité, dès lors que les responsabilités correspondantes se trouveraient énoncées à un niveau où elles seraient plus aisément consultables par toutes les parties prenantes dans le cadre de leurs attributions respectives. Rendre plus explicite, par ce processus d'intégration, le rôle que la cybersécurité est appelée à jouer dans le cadre des fonctions organiques et administratives peut réduire les malentendus et pallier le défaut d'appropriation. À titre d'exemple, les Inspecteurs ont pu constater l'existence, entre les spécialistes de la cybersécurité et les représentants d'autres unités institutionnelles, une certaine tension résultant de l'idée que les uns et les autres se faisaient de leurs contributions respectives à la constitution d'un solide dispositif de cybersécurité. **Dans ces circonstances, les Inspecteurs insistent sur le fait que les unités organiques, plus spécifiquement, doivent épouser davantage la cybersécurité en tant que dimension de leur activité.** Toutefois, la mise à contribution des unités administratives ne saurait signifier que toute la responsabilité leur revient en tant que pilotes du risque. De même que les spécialistes de la cybersécurité ne sauraient assumer seuls la responsabilité de la protection des actifs institutionnels, sans que les unités administratives n'endossent une part importante de cette charge. Il sera important de trouver le juste équilibre. L'intégration des considérations de cybersécurité dans l'ensemble des domaines institutionnels peut ouvrir la voie à la confirmation de ce qu'ils peuvent attendre les uns des autres ainsi que de leurs rôles respectifs à cet égard.

95. **Les formations en fonction du rôle doivent être développées.** Plusieurs entités participantes ont pour pratiques encourageantes de proposer des formations à la cybersécurité en fonction du rôle et de mettre en place des mesures de sensibilisation. Ces pratiques devraient être développées pour préparer au mieux toutes les parties prenantes à jouer le rôle attendu d'elles dans la cyberrésilience institutionnelle. Au niveau du système, le Réseau Technologies de l'information et des communications a déjà encouragé un travail similaire avec certains groupes d'utilisateurs selon leurs responsabilités fonctionnelles, qu'il s'agisse de spécialistes du progiciel de gestion intégré, des finances, de la comptabilité et des achats, ou de directeurs exécutifs. Certaines entités ont également mis au point des cours spéciaux à l'intention de membres du personnel qui, chargés de missions sensibles ou appelés à être déployés sur le terrain, feront face à des risques particuliers tenant au lieu ou à l'infrastructure de leur affectation. Parmi ces publics particuliers, il pourrait s'avérer utile d'accorder un degré de priorité élevé au personnel d'encadrement et de direction, d'une part, et aux responsables de programme, de l'autre, en ce que leur compréhension de la cybersécurité et leur attitude vis-à-vis de celle-ci est susceptible de se disséminer en cascade au sein de leurs entités ou unités respectives et d'y avoir un impact sensible sur l'épanouissement − ou non − d'une culture de la cybersécurité.

H. Importance du personnel en tant que première ligne de défense

96. **Le « facteur humain », à la fois menace, défense, élément essentiel de la culture de la cybersécurité et pilier de la résilience.** La majorité des entités des Nations Unies ont pris d'importantes dispositions technologiques et opérationnelles pour contribuer à la prévention et à l'atténuation du risque de cyberattaques (par. 38). Cependant, la communauté des spécialistes de la cybersécurité reconnaît que la nécessité d'instruire chaque membre du personnel sur son rôle dans la protection de l'information et des actifs numériques de son entité, ainsi que sur l'importance d'observer les règles, les procédures et les meilleures pratiques en matière de cybersécurité, reste un défi de taille. À bien des égards, le « facteur humain » a gagné en importance dans le paysage des menaces à la cybersécurité, comme l'atteste la préoccupation croissante que suscite parmi les entités participantes le constat que les utilisateurs finals individuels sont de plus en plus souvent la cible d'attaques de manipulation psychologique (par. 26 et 27). Ce facteur s'est également avéré particulièrement difficile à gérer en tant que source de risque. Outre qu'il est tout à la fois la première ligne de

défense et le lien le plus faible du filet de sécurité numérique de son entité, chaque membre du personnel représente aussi un pilier important de la résilience et de la culture de la cybersécurité institutionnelles. Les conséquences néfastes des mauvaises pratiques informatiques sont multiples et prennent souvent la forme de graves menaces internes. Celles-ci peuvent être causées par : des erreurs que commettent des utilisateurs peu attentifs ou peu concernés ; un manque de conscience ou de vigilance (souvent exploité par les attaques d'hameçonnage) ; de mauvaises pratiques de protection des données, comme le choix de mots de passe faibles ou le partage d'identifiants d'accès ; l'utilisation de logiciels non autorisés ou dépassés ; la mise au point d'applications en dehors des environnements informatiques gérés par l'entité ; les systèmes qui manquent de correctifs ou qui ont été négligemment entretenus. Ces pratiques restent les menaces les plus généralisées auxquelles les entités sont confrontées au quotidien. Il est manifestement impératif de donner aux utilisateurs les moyens de prendre une part active à l'amélioration de la cyberrésilience institutionnelle.

97. **L'aptitude à se servir des outils numériques, point de départ non négociable.** Condition préalable à toute compréhension des effets que la pratique individuelle de la cybersécurité peut avoir sur l'entité tout entière, l'alphabétisation numérique de chaque membre du personnel est un point de départ non négociable. Au XXIe siècle, la capacité de fonctionner dans la sphère numérique est obligatoire pour toute personne rattachée de quelque façon que ce soit à l'ONU ou à ses activités. L'utilisation confiante des équipements électroniques et applications ordinaires doit être acquise à tous les utilisateurs de l'infrastructure numérique des entités des Nations Unies − personnel, personnel affilié, experts en mission, représentants participant aux conférences ou toute autre personne qui se connecte aux ressources numériques internes ou les exploite. C'est seulement lorsque cette condition fondamentale est remplie que l'on peut entreprendre de rappeler aux employés que la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information et des actifs institutionnels fait partie intégrante du travail et des responsabilités de chacun. Le pas le plus difficile à franchir, toutefois, peut consister à passer de la prise de conscience des règles, responsabilités et outils de la cybersécurité ainsi que des consignes relatives aux pratiques informatiques saines, d'une part, à un changement de comportement durable et à une transformation des attitudes individuelles et collectives, d'autre part.

98. **L'importance de la formation est reconnue.** De solides programmes de formation et de sensibilisation sont un des moyens par lesquels les mentalités peuvent être amenées à évoluer vers la reconnaissance des cyberrisques et l'acquisition d'une saine pratique de la cybersécurité. Ce fait a été souligné dans la littérature spécialisée et dans les rapports des comités d'audit et de contrôle adressés à la direction exécutive de plusieurs entités des Nations Unies. Se présente alors un certain paradoxe : alors que les infrastructures et les systèmes sont souvent protégés par d'importants mécanismes techniques à plusieurs couches, la capacité de tous les membres du personnel d'en maîtriser l'utilisation serait quant à elle à la traîne, du moins dans certaines entités, si l'on en croit les responsables interrogés. Plus un système est robuste, plus le risque se déplacera vers ses utilisateurs, et ce risque sera d'autant plus grand que l'hygiène informatique de l'utilisateur laissera à désirer. Évoquant la sensibilisation à la cybersécurité, le Comité consultatif indépendant pour les questions d'audit auprès du Secrétariat de l'ONU a déclaré que « la méconnaissance de cette question pourrait entraîner des atteintes à la sécurité des systèmes d'information et de communication, à la confidentialité et à l'intégrité de l'information »[22].

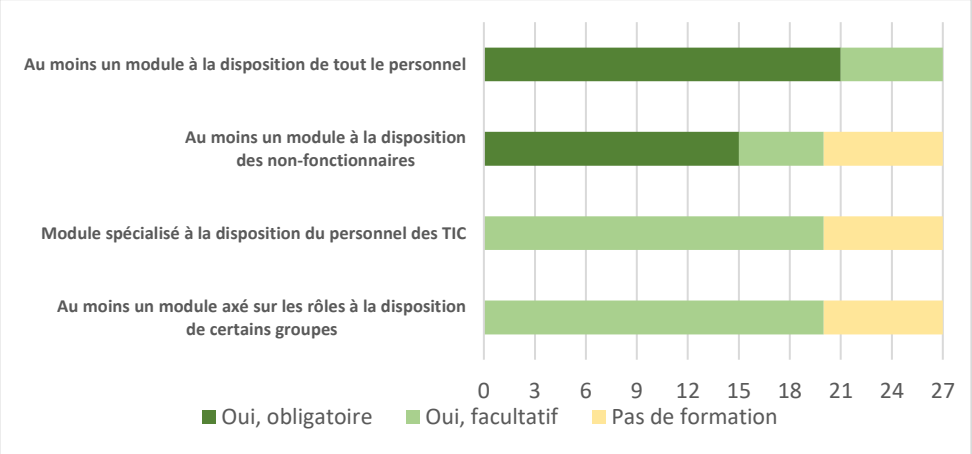
99. **Le relevé des possibilités de formation offertes au personnel est prometteur.** Le Réseau Technologie et numérique a dit, au fil des ans, l'importance des formations de sensibilisation à la sécurité de l'information, et les entités participantes ont déployé des efforts pour étoffer leur offre en la matière[23]. La figure VII présente les informations recueillies concernant quatre catégories de publics. Elle confirme l'existence de cours de formation obligatoires dans la majorité des entités, mais montre aussi que, dans certains cas, ces cours sont facultatifs. Ils portent habituellement sur le bon usage des comptes de messagerie, à des fins professionnelles plutôt que personnelles, sur le risque qu'il y a à ouvrir des pièces jointes d'origine inconnue, sur les consignes de sélection et d'utilisation des mots

[22] A/73/304, par. 51.

[23] Voir, par exemple, CEB/2011/3 (en anglais) et CEB/2018/HLCM/ICT/10 (en anglais).

de passe, et sur la consultation sécurisée des sites Web externes. Ces dernières années, les comités d'audit et de contrôle ont appelé l'attention des entités participantes sur la nécessité d'augmenter le taux de participation aux cours de formation obligatoires, ce qui va dans le bon sens en principe. Les Inspecteurs tiennent toutefois à souligner que la seule participation aux formations obligatoires n'est que rarement un indicateur utile du degré de sensibilisation atteint, ni d'ailleurs une garantie suffisante qu'un changement de comportement a effectivement été obtenu. Un indicateur plus pertinent, quoique probablement plus complexe à suivre et à analyser, pourrait être obtenu en comparant le nombre d'utilisateurs se livrant à des pratiques non recommandées (comme cliquer sur un lien ou une pièce jointe dans un message d'hameçonnage) à différents moments, en particulier avant et après une formation ou des interventions de sensibilisation. Certaines bonnes pratiques constatées en rapport avec les formations obligatoires consistent à imposer une date d'achèvement au personnel nouvellement recruté, de sorte à limiter le temps pendant lequel ce personnel est exposé à des risques accrus faute d'y avoir été sensibilisé, et à exiger du personnel en général qu'il suive annuellement des séances de remise à niveau afin de maintenir l'effet d'apprentissage au cours du temps.

Figure VII
Formations de sensibilisation à la sécurité de l'information en 2020, par modules de formation et entités participantes du CCI



Source : Questionnaire du CCI, 2020.

100. **Les dispositions à prendre pour les autres catégories de personnel et les utilisateurs occasionnels.** Environ la moitié des entités participantes ont également rendu la formation à la sécurité de l'information obligatoire pour d'autres catégories de personnel, tandis que l'autre moitié la proposent à titre de module facultatif ou n'ont pris aucune disposition à cet égard. Il est crucial de s'occuper des non-fonctionnaires. Les membres des catégories de personnel n'ayant pas la qualité de fonctionnaire sont souvent forcés, par les limites imposées aux ressources, d'utiliser leurs propres appareils pour se connecter à l'infrastructure institutionnelle. Sans compter que les utilisateurs qui ne font pas fréquemment usage des systèmes et infrastructures institutionnels risquent d'être moins au fait de l'usage correct et sûr qui doit en être fait, dans le respect des règles et pratiques de l'entité. L'absence de mécanismes coercitifs applicables aux personnes qui ne sont pas directement employées par l'entité et ne relèvent donc pas pleinement de son pouvoir disciplinaire peut encore réduire leur disposition à se conformer à des règles déjà peu respectées. Ces problèmes peuvent être accentués lorsqu'une entité fait largement appel à des consultants, des vacataires et du personnel engagé pour une période de courte durée. **Les Inspecteurs rappellent que les formations et les initiatives de sensibilisation doivent s'adresser à l'ensemble du personnel. Les menaces ne font pas de différence entre les utilisateurs. Les Inspecteurs proposent par conséquent aux entités qui n'ont pas rendu ces modules obligatoires de faire le nécessaire dans ce sens.**

101. **Les défis de la formation.** Les entités participantes ont signalé aux Inspecteurs une série de difficultés susceptibles d'affecter la bonne exécution des programmes de formation à la cybersécurité. Elles ont été plusieurs à relever les contraintes financières qui limitaient les formations qu'elles pouvaient concevoir et offrir, et même, dans certains cas particulièrement inquiétants, qui les obligeaient à réserver ces programmes à certaines catégories d'utilisateurs seulement. La question financière se pose d'autant plus que la matière évolue rapidement, par nature, et peut rapidement rendre obsolète le contenu d'un cours, auquel il faudra alors apporter des mises à jour ou des suppléments, souvent à grands frais. Un autre défi à relever est la lassitude face aux formations, susceptible de réduire l'efficacité des programmes. La situation peut encore gagner en complexité à cause d'un taux élevé de rotation du personnel ou d'un manque d'autorité sur certaines catégories de personnel. Les entités qui se déploient sur le terrain peuvent connaître des problèmes de formation particuliers, comme pour toutes les autres possibilités d'apprentissage. Cet aspect des choses n'a toutefois pas pu être étudié dans le cadre du présent examen. Enfin, les responsables de la cybersécurité ont relevé un manque général de mesures de coercition en cas de non-conformité aux exigences de formation, et mis en corrélation l'inefficacité possible de nombreux programmes de formation avec l'absence de sanctions, une lacune qui, dans les faits, revenait à rendre facultatives même les formations obligatoires. **Pour veiller à un meilleur respect des obligations de formation, les Inspecteurs proposent que les chefs de secrétariat envisagent d'établir un lien formel entre l'achèvement de la formation à la sécurité de l'information et d'autres procédures institutionnelles d'habilitation du personnel.** Il peut s'agir, par exemple, de conditionner l'habilitation de sécurité en vue d'un déploiement sur le terrain ou l'octroi et l'extension de droits d'accès aux systèmes de TIC à la preuve de l'achèvement de la formation nécessaire, y compris lorsqu'il s'agit d'un cours de remise à niveau. Un précédent existe déjà en ce qui concerne les considérations de sûreté physique précédant un voyage en mission, l'autorisation de voyager dépendant de l'achèvement du cours de base de sécurité sur le terrain, faute de quoi elle sera refusée.

102. **Les initiatives de sensibilisation dans le système des Nations Unies.** Il existe dans le système des Nations Unies de multiples initiatives de sensibilisation relatives aux activités en ligne qui portent sur les cyberrisques et les mesures recommandées pour y faire face. C'est le cas, par exemple, de la semaine d'octobre consacrée à la sécurité de l'information, une initiative à laquelle se joignent plusieurs entités autour du monde et qui comprend des activités interactives, des jeux et des séances d'information. Les programmes du Bureau international du Travail (BIT) et de l'OMPI ont été reconnus, certains dans le cadre d'audits externes, comme particulièrement innovants et efficaces. Il serait également intéressant de consacrer des séances de sensibilisation aux cyberrisques de la sphère privée (comme ceux qui concernent les enfants ou les photos de famille prises contre rançon) dans l'espoir que cet aspect de la question suscitera plus d'intérêt et que les leçons qui en seront tirées déteindront sur la sphère professionnelle. Certaines entités organisent pour les nouveaux membres de leur personnel des séances d'information menées en présentiel par le responsable de la sécurité de l'information, tandis que d'autres consolident les leçons apprises en diffusant de courts messages vidéo aux utilisateurs qui ont été victimes d'une cyberattaque. Les simulations de campagnes d'hameçonnage figurent parmi les moyens de sensibilisation les plus populaires et leurs résultats semblent avérés (encadré 5).

Encadré 5
L'utilité des campagnes de simulation d'hameçonnage

L'hameçonnage (ou *phishing*) consiste à envoyer des messages électroniques prétendant provenir d'une source fiable afin d'amener les destinataires à révéler des renseignements sensibles. Les pirates utilisent ensuite ces renseignements pour accéder frauduleusement aux systèmes de l'entité à des fins de gains financiers ou de perturbation.

Les campagnes d'hameçonnage simulées imitent les procédés des hackers pour détecter les utilisateurs qui sont plus susceptibles d'être trompés et de cliquer sur des liens malveillants ou d'ouvrir des pièces jointes infectées. Ces simulations sont également utilisées pour vérifier les compétences acquises dans le cadre des formations. Pour être les plus efficaces possibles, elles devraient être accompagnées de services orientés vers les utilisateurs, comme un point de contact bien apparent et des procédures simples et connues de tous pour le signalement de messages électroniques suspects. Certaines entités participantes ont prévu un système qui permet de signaler les messages d'hameçonnage en cliquant sur un bouton directement disponible dans la messagerie électronique du personnel.

Les chiffres communiqués aux Inspecteurs attestent l'utilité de ces campagnes d'hameçonnage simulées, les responsables de la sécurité de l'information ayant généralement constaté une réduction du pourcentage d'utilisateurs qui ouvrent des messages et des pièces jointes suspectes à l'issue de campagnes successives. À titre de contexte, certains responsables de la cybersécurité situent aux environs de 5 % la part habituellement considérée comme acceptable de la main-d'œuvre qui ne se conforme pas aux règles de cybersécurité.

Les simulations de campagnes d'hameçonnage sont fréquemment lancées dans le cadre plus large des tests d'intrusion. Ces tests, souvent appelés « *pen* » en anglais (abréviation de « *penetration testing* ») sont constitués d'une série d'exercices pratiques qui visent le réseau, les systèmes et les ressources humaines de l'entité pour repérer les vulnérabilités, mesurer le niveau de conformité aux règles et procédures, et évaluer l'efficacité des défenses et des procédures de reprise.

103. **Une transition des modules de formation vers un programme de sensibilisation cohérent.** En remplacement de la pratique actuelle qui consiste à fournir des modules de formation séparés à tout un chacun, sans véritable projet stratégique, **les Inspecteurs conseillent aux entités de s'orienter vers la conception d'un programme complet de formation et de sensibilisation doté d'objectifs clairement définis pour chaque catégorie de parties prenantes, selon les risques auxquels elle pourrait exposer l'entité.** L'adoption d'un tel modèle permettrait aux entités de ne plus dépendre des taux de participation comme indicateurs de conformité aux règles, mais de faire de la formation un outil dynamique de changement de la culture interne en matière de cybersécurité. Idéalement, un tel programme devrait être exécuté au moyen de méthodes innovantes combinant diverses approches et messages en fonction de chaque public. Pour renforcer le sentiment d'appropriation et stimuler l'apprentissage dans ce domaine, les entités pourraient également envisager de mettre en place un système de groupes d'appui constitués de pairs, et de désigner des individus qui, dans chaque service, pourraient être formés en tant que personnes-ressources pour le programme et fournir à ce titre une assistance pratique aux autres membres du personnel, quand et où le besoin s'en fait sentir.

I. Affectation optimale de ressources financières à la cybersécurité

Estimer le niveau actuel des ressources consacrées à la cybersécurité

104. **Les ressources de cybersécurité au sein du système des Nations Unies sont généralement moindres qu'à l'extérieur, tout en étant difficilement quantifiables.** C'est presque un lieu de commun de dire que les entités des Nations Unies ont moins de ressources à consacrer aux TIC en général et à la cybersécurité en particulier que les entités de taille comparable des secteurs public et privé. Il est cependant difficile de quantifier ce

fossé en termes absolus comme relatifs. Selon une estimation, par exemple, moins de 1 % des dépenses de l'ONU est consacré aux TIC, et moins de 1 % de cette quote-part est réservé à la sécurité de l'information, alors que la moyenne industrielle est d'environ 7 %[24]. Soucieux de dresser un tableau de la situation fondé sur les faits, le CCI a mené une enquête auprès de ses entités participantes sur la question de l'allocation de ressources aux TIC et à la cybersécurité. Comme on pouvait peut-être s'y attendre, les Inspecteurs sont arrivés à la même conclusion que celle qui figurait dans le compte rendu du symposium du Groupe d'intérêt pour la sécurité informatique en 2018, à savoir que les chiffres restaient nébuleux pour le système tout entier.

105. **Estimer les dépenses de cybersécurité est à la fois complexe et utile.** Plusieurs facteurs rendent difficile le calcul des ressources dont dispose la cybersécurité. Ses coûts (encadré 6) ne sont généralement pas répertoriés séparément sous tel poste budgétaire ou telle catégorie de dépenses. Leur financement peut relever d'un ou plusieurs postes (par exemple, les dépenses de fonctionnement, les dépenses de personnel ou les dépenses d'infrastructure ou d'équipement) ou domaines thématiques (par exemple, dans l'enveloppe des TIC ou en dehors de celle-ci). La difficulté de trouver des informations concernant les ressources et les dépenses de la cybersécurité dans plusieurs documents budgétaires et états financiers est accrue par la diversité des structures budgétaires, comme l'atteste la coexistence de budgets ordinaires et de contributions volontaires (extrabudgétaires), qui peuvent inclure des fonds d'équipement autonomes destinés à de grands projets d'infrastructure. Plusieurs entités font également la différence entre les dépenses d'équipement (non récurrentes) et les dépenses de fonctionnement (récurrentes), ce qui vient encore nuancer le tableau. Il a même été constaté dans une entité qu'une grosse part des ressources destinées aux TIC se répartissaient entre les budgets-programmes d'unités administratives qui disposaient de capacités informatiques. Sur cette toile de fond, il est pour ainsi dire impossible de faire quelque déclaration fiable que soit sur les ressources totales mises à la disposition de la cybersécurité. En tout état de cause, la complexité de l'exercice serait disproportionnée par rapport à son utilité : le niveau des ressources affectées à la cybersécurité dans une entité n'est qu'une valeur indicative limitée pour ce qui est du niveau de protection assuré.

Encadré 6
Coûts de la cybersécurité

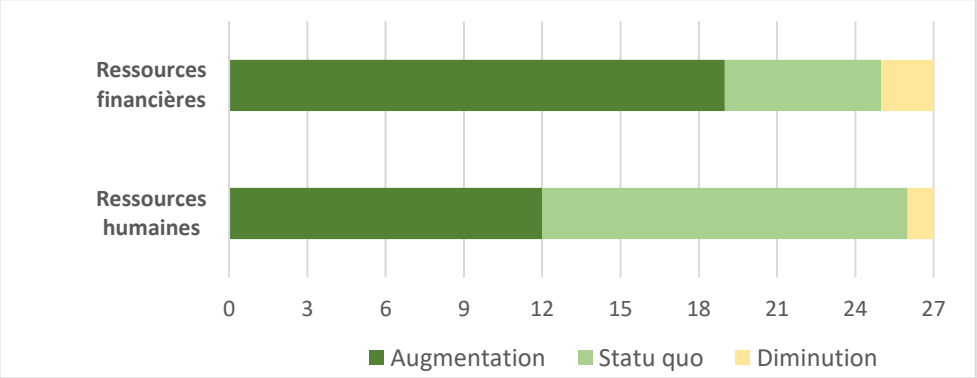
- **Coûts directs.** Les coûts évidents (directs) de la cybersécurité vont des dépenses de personnel (personnel et prestataires externes) et d'infrastructure, tels les achats de matériel et de logiciels (dépenses d'équipement et de maintenance et droits d'exploitation des logiciels), aux services (tels les abonnements aux renseignements sur les menaces et les services en sous-traitance de fournisseurs commerciaux et du CIC). Les proportions de ces dépenses varient et reflètent le rapport entre capacités internes et sous-traitance choisi par chaque entité.
- **Coûts indirects.** Il y a d'autres coûts (indirects) à prendre en compte pour établir la facture de la cybersécurité. En fait, on tend à associer une ponction financière importante aux mesures prises pour contrôler les dégâts à la suite d'un incident, notamment pour mobiliser les capacités spéciales nécessaires au rétablissement des services perturbés, corriger les vulnérabilités nouvellement révélées, faire face à la perte de productivité pendant que les systèmes sont hors service, former le personnel pour mieux prévenir les intrusions et y riposter et pour garder à jour les capacités spécialisées (humaines comme technologiques.

106. **La tendance récente est à l'augmentation du financement, mais au maintien des contraintes affectant les capacités.** Les Inspecteurs relèvent que la plupart des entités participantes ont signalé une augmentation des ressources affectées à la cybersécurité ces dernières années (fig. VIII). À première vue, la tendance peut paraître prometteuse. Le diagramme fait cependant ressortir que l'augmentation rapportée des ressources financières allouées à la cybersécurité ne s'est pas automatiquement traduite par une

[24] CEB/2018/HLCM/ICT/4 (en anglais).

augmentation des ressources humaines. En fait, la grande majorité des entités participantes ont indiqué que le niveau actuel de ressources restait un obstacle à la mise en place d'un cadre de cybersécurité performant. Une des entités a même déclaré que le coût de sa protection contre les menaces croissantes qui pesaient sur sa cybersécurité avait triplé au cours des deux derniers exercices biennaux. Selon les évaluations des entités elles-mêmes, le manque de ressources avait touché le plus durement les moyens humains et la disponibilité de spécialistes internes, la capacité d'investir suffisamment dans l'infrastructure informatique et de communication et la capacité de remplacer les applications obsolètes. En outre, dans celles des entités qui manquent cruellement de ressources ou dont les budgets ont cessé de croître, les ressources nouvellement consacrées à la cybersécurité pourraient être le résultat d'un redéploiement interne, peut-être au détriment d'autres investissements qui étaient principalement, mais pas exclusivement, destinés aux TIC. Face à cette situation qui risque de ne pas être viable à terme, les Inspecteurs sont préoccupés par le fait que les ressources disponibles, même là où elles ont augmenté, pourraient avoir été distancées par la sophistication technologique des attaquants et la généralisation des TIC dans les activités des entités des Nations Unies. Comme il a été très justement dit dans le cadre du Groupe d'intérêt pour la sécurité informatique, la dépendance grandissante vis-à-vis des services faisant appel à l'informatique n'a pas été contrebalancée par une augmentation des ressources de la fonction de sécurité de l'information[25].

Figure VIII
Évolution des ressources de la cybersécurité, selon les informations fournies par les entités participantes du CCI (2015-2020)



Source : Questionnaire du CCI, 2020.

107. **Sources de financement.** Selon les informations recueillies, les ressources consacrées à la cybersécurité dans la plupart des entités participantes proviennent principalement du budget ordinaire, tandis que certaines entités s'appuient sur une combinaison de ressources ordinaires et extrabudgétaires, et très peu sur les secondes exclusivement. La prévisibilité relative des ressources budgétaires ordinaires peut certes s'avérer favorable à la durabilité des capacités de cybersécurité, mais c'est une formule qui ne saurait se passer de la planification stratégique nécessaire pour que les ressources prévues deviennent disponibles au moment voulu. Les ressources extrabudgétaires peuvent quant à elle autoriser une plus grande flexibilité et s'avérer plus attrayantes pour les donateurs souhaitant réserver leurs contributions à la cybersécurité. Une poignée d'entités disposent d'un fonds spécial qui, soit est consacré à l'infrastructure informatique et de communication (OMS), soit peut être mis à contribution pour de grands projets institutionnels (OMPI et AIEA). Comme évoqué en rapport avec les feuilles de route établies par les entités à plus long terme pour améliorer leurs cadres de cybersécurité, les investissements dans ce domaine tendent à être pluriannuels par nature. Il s'ensuit que les cycles budgétaires actuels peuvent tout à la fois manquer d'envergure pour que les considérations stratégiques à long terme puissent prendre pied et manquer de souplesse pour autoriser le déploiement rapide de fonds requis pour répondre aux exigences ponctuelles et à court terme qui peuvent survenir dans un domaine technologique et un paysage de menaces aussi trépidants que ceux de la cybersécurité.

[25] Ibid.

C'est une lacune que peuvent combler les fonds spéciaux, pour autant que le permettent les principes de gouvernance et les modalités et conditions d'affectation qui les régissent, comme convenu par les organes délibérants et directeurs.

Vers l'optimisation des investissements dans la cybersécurité

108. **Les demandes de ressources adressées aux organes directeurs doivent être étayées par un dossier de décision.** Il va de soi que les entités ne sauraient s'attendre à ce que les demandes d'affectation de ressources adressées aux organes directeurs soient accueillies sans justification en bonne et due forme du fait que les investissements dans la cybersécurité devraient prendre le pas sur d'autres dépenses institutionnelles. **Comme point de départ, les Inspecteurs recommandent que les demandes de ressources soient étayées par une analyse approfondie des risques et un dossier de décision précisant les coûts, avantages, risques et économies escomptées, en renvoyant aux retombées financières possibles d'un renoncement à l'investissement envisagé.** Cette façon de procéder sera d'autant plus efficace qu'elle se doublera d'un projet de mise en œuvre et de calendrier, sous la forme, par exemple, d'une feuille de route, comme préconisé ailleurs dans le présent rapport, et qu'elle donnera lieu à des états d'avancement réguliers. Les Inspecteurs constatent que lorsque les directions exécutives ont soumis des dossiers de décision convaincants, énonçant un objectif clair et des critères d'amélioration, et démontré l'aspect critique de l'investissement, les organes directeurs étaient généralement plus disposés à appuyer le projet en lui affectant des ressources propres. C'est ce qui s'est produit ces dernières années, notamment dans des entités telles que l'OACI, le BIT, le HCR et l'OMPI, et c'est une pratique encourageante si on considère qu'en toute probabilité, les menaces toujours plus sophistiquées qui pèsent sur la cybersécurité continueront de nécessiter non pas moins, mais plus de ressources.

109. **Les dépenses de cybersécurité peuvent et doivent être optimisées.** Il va sans dire qu'un cadre de cybersécurité solide et bien protégé a un coût, et que si les entités des Nations Unies tiennent à protéger leurs informations, systèmes et actifs numériques, elles n'ont d'autre choix que de doter leurs dispositifs des ressources nécessaires. Les tentatives de déterminer le niveau des ressources à réserver à la cybersécurité sur la base d'un pourcentage des budgets institutionnels consacrés aux TIC n'ont pas produit de résultats intéressants. Le parti d'exprimer l'adéquation des ressources en termes monétaires ne doit pas être sacralisé. L'argent seul ne saurait résoudre le problème. Gartner résume la chose sans détours : le montant consacré à la cybersécurité ne reflète pas le niveau de protection[26]. La question qui compte en matière de cybersécurité n'est pas tant de savoir combien dépenser, mais où allouer les ressources le plus utilement possible. Les réponses faites aux questionnaires du CCI font ressortir des incohérences dans la façon dont les priorités de financement de la cybersécurité sont établies et, par suite, un risque accru d'inefficacité dans l'utilisation de ressources déjà rares. Un moyen convaincant, quoique relativement complexe et nécessitant un assez lourd travail d'adaptation, d'optimiser les investissements de cybersécurité consiste à suivre un processus rigoureux tel que la méthode Sherwood Applied Business Security Architecture (ou un outil équivalent), fondée sur le principe de traçabilité bidirectionnelle. L'architecture de sécurité d'entreprise est constituée de telle sorte que chaque exigence opérationnelle se voit associer au moins un contrôle de sécurité et que chaque contrôle de sécurité correspond en retour à une exigence de sécurité opérationnelle déclarée[27]. L'OMPI utilise déjà cette méthode, qui a également été abordée dans le cadre du Groupe d'intérêt pour la sécurité informatique, et **les Inspecteurs sont d'avis qu'elle mérite d'être examinée plus avant comme moyen d'ancrer solidement les investissements en matière de cybersécurité dans les exigences opérationnelles et dans de saines pratiques de gestion des risques, tout en maintenant des liens solides entre les premiers et les secondes, et d'éviter par là de consacrer trop ou trop peu de ressources à une fonction essentielle pour la continuité des opérations.**

[26] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, février 2020.

[27] De plus amples renseignements sur la méthode Sherwood Applied Business Security Architecture sont disponibles à l'adresse https://sabsa.org/sabsa-executive-summary (en anglais).

Encadré 7
Les possibilités avantageuses des solutions *open source*

Les logiciels *open source* sont conçus et diffusés selon un modèle qui forme désormais partie intégrante du secteur des TIC. Certains outils basés sur ces logiciels sont largement utilisés dans le domaine de la cybersécurité, notamment pour communiquer des renseignements sur les menaces, gérer les identités et les accès, analyser les réseaux, détecter et prévenir les intrusions, riposter aux incidents et rechercher des preuves. Certains logiciels *open source* sont même reconnus comme des ressources de premier plan dans leurs catégories respectives.

Bien qu'il ressorte des réponses aux questionnaires du CCI que certaines entités participantes complètent déjà leurs solutions commerciales et maison par des logiciels *open source*, il peut y avoir d'autres possibilités d'exploitation de ces outils par les entités des Nations Unies. Ils peuvent constituer des solutions valables, en particulier dans des entités qui disposent de faibles ressources pour fonctionner.

Comme dans le cas de tout produit propriétaire, les solutions *open source* devraient être évaluées sur la base de leur valeur propre. Il est toutefois certains avantages à caractère général fréquemment associés aux produits *open source* bien entretenus, comme la transparence, la sécurité, l'économie des frais de licences et des droits, l'utilisation de normes ouvertes et le faible risque de dépendance vis-à-vis d'un fournisseur.

Bien que l'utilisation de logiciels *open source* n'entraîne pas, normalement, de frais de licences, elle n'en est pas totalement dénuée de coût pour autant. Son installation, sa configuration et sa maintenance, de même que la maîtrise technologique que ces opérations nécessitent, se traduisent en temps de main-d'œuvre et représente donc un coût. Le coût total effectif de l'utilisation de telles plateformes peut ne pas apparaître clairement aux entités dont les ressources techniques sont limitées et qui n'ont guère l'expérience du déploiement de de telles applications, quoique cette réserve vaille − à divers degrés − pour les produits commerciaux aussi.

Les entités ont d'autres choix que de se cantonner à des formules exclusivement propriétaires ou exclusivement *open source*. Il existe des produits conçus selon un modèle hybride, pour tirer parti de ce que les deux formules ont de mieux à offrir, à savoir la liberté et la transparence de l'approche *open source* et l'appui structuré fourni par les fournisseurs empressés. Une autre possibilité consiste à utiliser à la fois des logiciels propriétaires et des logiciels *open source* en les destinant à différentes fonctions et finalités au sein de l'entité.

J. Investissement dans des ressources humaines spécialisées

La fonction de sécurité de l'information n'est pas présente dans toutes les entités participantes

110. **Les responsabilités associées à la cybersécurité vont au-delà de la spécialisation technique.** La majorité des entités participantes ont investi dans le recrutement de ressources humaines spécialisées pour prendre en charge les différentes dimensions de la cybersécurité, parfois en les plaçant sous la direction d'un responsable de la sécurité de l'information. Les éléments centraux relevant de la fonction associée consistent à élaborer des mesures de contrôle au niveau opérationnel, d'une part, et à donner des orientations de gestion au niveau stratégique, d'autre part, dans le but de réaliser les objectifs de protection attribués à la cybersécurité selon la définition retenue dans le présent rapport. Dans ce sens, la fonction a une portée qui dépasse la sphère numérique et ne se limite pas à fournir un savoir-faire technique. Elle concerne notamment les tâches suivantes : mettre au point et diffuser un cadre réglementaire institutionnel (orientation et communication) ; donner des conseils sur la manière de définir et de gérer les risques (gestion des risques) ; collaborer avec les unités administratives à l'évaluation des risques et à l'analyse d'impact sur les opérations (coordination et analyse) ; enquêter sur les atteintes importantes (capacités d'enquête et d'analyse) ; recommander et apporter les améliorations nécessaires aux mesures de contrôle (connaissances opérationnelles et techniques)[28]. Telles qu'elles sont décrites, ces tâches ont

[28] Voir SFIA Foundation, *Skills Framework for the Information Age (SFIA) 7*, 2018.

une dimension d'encadrement, à la fois dans le cadre des TIC et en dehors de celui-ci, et elles doivent s'accomplir en étroite collaboration avec une vaste gamme de parties prenantes, en particulier les unités administratives. L'autorité qui est déléguée au responsable de la sécurité de l'information (et aux spécialistes de la cybersécurité plus généralement) de communiquer avec les composantes de l'entité et d'obtenir d'elles qu'elles agissent de telle ou telle façon est par conséquent cruciale.

111. **Les capacités internes varient.** Selon les recherches effectuées par le CCI, au moins 16 entités participantes se sont dotées de capacités internes en ressources humaines spécialisées et exclusives allant d'un unique fonctionnaire de la sécurité de l'information, parfois même affecté à temps partiel, à une unité administrative plus étoffée sous la direction d'un responsable (responsable en chef, responsable principal) de la sécurité de l'information, généralement de classe P-4 ou P-5 (voir annexe V). Par contre, dans 10 entités participantes, les tâches relevant de la cybersécurité sont assurées principalement par des fonctionnaires des services chargés des TIC, en même temps que leurs autres fonctions. Le recours à des spécialistes externes est fréquent en raison de la nature techniquement complexe d'un domaine en constante évolution nécessitant un degré de spécialisation considérable qu'il est difficile et coûteux de maintenir à disposition et à niveau de façon permanente. Un complément de spécialisation est donc souvent obtenu en recrutant des ressources temporaires, notamment des consultants et des vacataires, ou en s'abonnant aux services de fournisseurs commerciaux ou du CCI. Certains interlocuteurs ont fait remarquer que la pénurie mondiale de praticiens expérimentés de la cybersécurité faisait partie des principales difficultés que les entités des Nations Unies rencontraient dans la mise sur pied, le fonctionnement et la gestion de leurs programmes de cybersécurité. Les Inspecteurs souhaitent attirer l'attention des entités qui ne sont pas en mesure de créer une fonction à part entière dans l'immédiat sur la solution de remplacement que constitue le service du CIC intitulé « *security governance* » (gouvernance de la sécurité), parfois aussi appelé « *chief information security officer as a service* » (responsable de la sécurité de l'information en tant que service), auquel sont actuellement abonnées six entités participantes et que quatre autres ont utilisé par le passé. **Les Inspecteurs sont d'avis que les entités des Nations Unies doivent recourir à une véritable planification de leurs ressources pour prévoir les connaissances spécialisées dont elles auront besoin dans le domaine de la cybersécurité à l'avenir, compte tenu en particulier du fait que les connaissances, compétences et aptitudes nécessaires pour remédier aux risques et aux difficultés de la cybersécurité sont spécifiques et peuvent ne pas être faciles à attirer et à conserver**.

112. **L'investissement dans des capacités propres mérite d'être envisagé.** S'il est vrai que les dispositions institutionnelles d'une entité devraient refléter sa taille ainsi que les exigences qui lui sont propres au regard d'une évaluation des risques et du cyberenvironnement dans lequel elle fonctionne, d'autres facteurs peuvent s'avérer plus décisifs. Les disparités que les Inspecteurs ont constatées entre les entités participantes en ce qui concerne leurs arrangements internes pourraient être davantage à l'image de leurs limitations que de choix délibérés ou stratégiques. De fait, dans quatre d'entre elles, la fonction de cybersécurité pouvait tout au plus être considérée comme naissante, un fait qui pourrait, de façon indirecte, mettre tout le système en danger. **Les Inspecteurs estiment que le fait de disposer d'un savoir-faire propre et spécialisé en matière de cybersécurité au sein de chaque entité contribue à renforcer le dispositif non seulement de l'entité en question, mais aussi du système tout entier, et qu'il s'agit par conséquent d'un investissement qui en vaut la peine.** Comme pour les autres fonctions associées aux activités de base des entités, la constitution à titre durable de capacités en ressources humaines internes pour la protection de l'information et des actifs numériques, lorsqu'elle est possible, est généralement préférable au recours récurrent à des ressources temporaires, d'autant plus que leur utilisation en soi et le pouvoir de coercition limité dont les entités disposent sur le personnel affilié (par. 100) représentent des risques supplémentaires. En outre, **la création d'un poste régulier de responsable de la sécurité de l'information chargé de la supervision et de la gestion de ce savoir-faire spécialisé peut être porteuse de l'attention et de la cohérence que requiert la cybersécurité et contribuerait, de l'avis des Inspecteurs, à renforcer la cyberrésilience des entités concernées.**

113. **Il n'existe pas de niveau et de rattachement hiérarchique communément admis pour la cybersécurité.** Le niveau hiérarchique le plus approprié pour la cybersécurité est une question qui a été débattue au sein du système des Nations Unies et au-delà, et qui n'a pas reçu de réponse définitive universellement applicable. Les normes internationales ne fournissent pas de consignes qui fassent autorité en la matière et laissent à chaque entité le soin de placer la fonction selon ses besoins et son architecture. Dans la majorité des entités des Nations Unies, elle se situe au sein du service des TIC, ce qui se traduit souvent par un rattachement hiérarchique direct au chef de ce service. Cet agencement structurel prédominant, s'il peut être considéré comme un héritage du passé, reflète aussi une réalité, à savoir que la cybersécurité tend à graviter naturellement vers les TIC, eu égard au sens de la technologie et au savoir-faire spécialisé requis pour gérer les systèmes informatiques et autres infrastructures de protection concernées. À cela s'ajoute que comme le service des TIC est souvent celui qui conçoit et applique les mesures opérationnelles de riposte en cas de cyberattaque, désolidariser les deux fonctions peut conduire à des pertes d'efficacité.

114. **La gestion des priorités institutionnelles divergentes entre les fonctions des TIC et de la cybersécurité.** Mis à part ce qui précède, le parti de placer le fonctionnaire ou l'équipe chargée de la cybersécurité sous l'autorité du chef des TIC peut créer des tensions entre les objectifs principaux de chaque rôle, la gestion des risques et la sécurité de l'information étant la préoccupation essentielle du premier, alors que le second s'intéresse avant tout à l'efficacité opérationnelle, au rapport coût/efficacité et à la rapidité de service. Les conflits d'intérêts potentiels sont aussi évidents que difficiles à résoudre. Une conception de la cybersécurité qui serait dominée par des considérations opérationnelles (que l'on s'attend souvent à trouver parmi les informaticiens) peut conduire, à terme, à la multiplication des effets négatifs sur les prestations fournies, lorsque des cyberrisques dont on ne se serait pas occupé plus tôt viendraient à se matérialiser. En revanche, une attitude trop axée sur l'évitement du risque (comme celle que l'on pourrait s'attendre à trouver parmi les spécialistes de la cybersécurité) pourrait entraîner une réduction excessive de l'agilité opérationnelle et entraver l'exécution du mandat d'autres façons. La gestion et la résolution des tensions entre différents objectifs institutionnels, et plus spécifiquement de leurs implications en matière de ressources, font partie des activités quotidiennes de tout responsable ; les directions exécutives sont les mieux placées pour trouver le juste équilibre à cet égard.

115. **Une fonction de cybersécurité qui a droit au chapitre.** Indépendamment du rattachement institutionnel de la cybersécurité, **les Inspecteurs insistent sur l'importance de donner aux considérations de cybersécurité l'occasion d'être exprimées et entendues par les décideurs compétents, sans restriction.** La fonction devrait être située là où elle peut s'adresser de façon autonome à l'équipe dirigeante et apporter une contribution effective à d'autres cadres institutionnels, tels que la gestion du risque institutionnel, la gestion de l'information et du savoir, la sûreté et la sécurité physiques et le contrôle, comme il est fait valoir tout au long du présent rapport. Ce résultat est obtenu le plus efficacement lorsqu'existe au sein de l'entité un solide mécanisme multipartite de gouvernance réunissant tous les services. L'OMPI et l'OACI, par exemple, disposent de mécanismes de gouvernance multipartites et multiniveaux bien conçus.

116. **Une formation spécialisée.** Quelles que soient les épaules sur lesquelles repose la cybersécurité au sein d'une entité, que la fonction soit assurée par une seule personne ou par une équipe, ou encore qu'elle soit répartie entre plusieurs ressources à temps partiel, il est important qu'une formation spécialisée reste à la disposition de tout le personnel des services chargés des TIC dont les responsabilités touchent à la sécurité, de sorte que leur savoir-faire et leurs compétences soient continuellement mises à jour. Selon les informations reçues, une telle formation destinée aux spécialistes des TIC, notamment aux administrateurs de systèmes et aux concepteurs, est déjà disponible dans la plupart des entités et doit continuer d'être encouragée (fig. VII). Un solide programme de formation à la cybersécurité et, là où c'est nécessaire, un processus de certification à l'intention de certains fonctionnaires spécialisés dans les TIC devraient idéalement constituer une composante de base du plan de travail des services concernés, et pouvoir s'appuyer sur un budget qui est acquis. Sans le bénéfice de ressources réservées à la mise à niveau continue des compétences, le personnel des services chargés de l'informatique et des communications doit entretenir ses connaissances de sa propre initiative ou en participant à des communautés professionnelles.

Cette solution, trop dépendante de la conscience professionnelle des individus, risque de ne pas être viable. Les Inspecteurs saluent l'intention déclarée de plusieurs entités de renforcer leur position dans ce domaine, non sans relever que, même là où le niveau des ressources permet ces formations spécialisées, elles sont la plupart du temps organisées de façon ponctuelle, sans objectifs à long terme ou d'approche systématique. Lorsque n'existent pas de capacités en ressources humaines affectées en permanence à la gestion de la cybersécurité, la bonne formation des membres du personnel chargé d'effectuer les tâches voulues est d'autant plus importante.

Un centre des opérations de sécurité pour une riposte opérationnelle cohérente en matière de cybersécurité

117. **Les principales fonctions du centre des opérations de sécurité.** Le centre des opérations de sécurité est une unité administrative qui se consacre aux opérations de cybersécurité au quotidien. Bien qu'il y ait d'inévitables différences entre ses diverses versions, lorsqu'il est investi du mandat le plus large, il est chargé de surveiller la sécurité d'une entité en prenant des mesures de prévention, de détection, d'analyse et de riposte face aux incidents de cybersécurité. Les spécialistes de la cybersécurité disent souvent qu'un centre des opérations de sécurité est fait de personnes, de moyens technologiques et de processus, et qu'il fonctionne en tant que centre nerveux où se collectent, se mettent en corrélation et s'analysent des flux d'informations provenant de diverses sources en temps réel. Les informations internes collectées par le centre peuvent comprendre des données provenant de sources telles que des appareils en réseau, des serveurs et des applications hébergées, des ordinateurs de bureau et des appareils portables, des systèmes de sécurité physique et des dispositifs de sécurité spécialisés. Le centre des opérations de sécurité collecte et traite également des renseignements externes concernant les menaces, habituellement une combinaison de renseignements *open source* (informations gouvernementales publiques comprises) et commerciales, qui sont alors mises en corrélation avec les données internes et analysées pour détecter tout signe de menace amorcée. Étant donné la complexité des tâches et la diversité des connaissances spécialisées nécessaires, la mise en place et l'exploitation d'un centre des opérations de sécurité tout à fait équipé et fonctionnel peut s'avérer une entreprise complexe et coûteuse. La nécessité d'un tel centre et, le cas échéant, l'opportunité de le monter en interne ou de faire appel à un fournisseur externe sont des questions auxquelles il appartient à chaque entité de répondre à la lumière de ses besoins propres.

118. **Les entités recourent à une variété de solutions internes, externes ou hybrides, pour s'équiper de centres des opérations de sécurité.** Les opinions divergent parmi les entités participantes quant aux avantages et aux inconvénients respectifs des formules internes et externes. Fait attesté par la diversité des installations et des pratiques que les Inspecteurs ont pu constater à l'occasion de leur examen. Certaines entités utilisent un centre des opérations de sécurité virtuel ou distribué, en ce sens que certaines de ses fonctions sont réparties parmi les membres d'un pool de ressources en personnel. Un certain nombre d'entités ont pris la décision de construire leur propre centre, de conception interne, tandis que d'autres utilisent une configuration acquise auprès de fournisseurs commerciaux ou partagent un centre avec d'autres entités par l'entremise du service correspondant du CIC, soit exclusivement, soit en combinaison avec un noyau de capacités internes. Les entités qui exploitent ces solutions hybrides ont, dans certains cas, établi une ligne de démarcation entre les fonctions stratégiques et relatives au contrôle institutionnel, qui restent du ressort interne, et le contrôle opérationnel qui, surtout lorsqu'il nécessite des capacités de surveillance 24 heures par jour et sept jours par semaine, est confié à des fournisseurs externes. Quelques-unes vont même jusqu'à utiliser plus d'un centre de sécurité, ce qui leur permet de séparer certaines portions de données particulièrement sensibles des ensembles destinés à être gérés par des services externes. Les Inspecteurs ont remarqué que quelques entités participantes envisageaient la possibilité de créer un centre des opérations de sécurité.

119. **Les éléments considérés dans le choix d'un centre des opérations de sécurité.** Parmi les arguments en faveur d'un centre interne figure la capacité de réagir plus rapidement aux menaces et de mieux contrôler les appareils finals, à un coût assurément plus élevé. Le contrôle amélioré tiendrait à ce que les appareils en question et leur situation seraient plus visibles, et qu'il serait de ce fait possible de remédier en temps réel à un risque qui se manifesterait à ce niveau. Le centre interne est aussi considéré comme un moyen efficace de

centraliser les fonctions de cybersécurité, ce qui, selon un large consensus au sein du secteur, conduit à une résilience globale accrue. Pour de nombreuses entités des Nations Unies, le coût de fonctionnement d'un centre interne des opérations de sécurité peut s'avérer prohibitif, à en juger par les informations disponibles, tandis que les avantages à en tirer peuvent ne pas être en proportion avec le profil de cybersécurité de ces entités et leurs exigences de protection correspondantes. Seul un petit nombre d'entités des Nations Unies peuvent se permettre d'exploiter un programme de cybersécurité complet pour s'occuper des menaces et y riposter de façon autonome, en s'appuyant uniquement sur des capacités internes. Qui plus est, même si elles arrivent à mettre en place les structures nécessaires, elles peuvent encore échouer à soutenir un effectif permanent et disponible sur demande constitué de spécialistes de la cybersécurité aux multiples compétences, capables de riposter à des cyberattaques complexes qui tendent à être peu fréquentes et irrégulières, et qui supposent donc une fluctuation du personnel requis. Certaines entités considèrent en outre que la réalisation de toutes les tâches opérationnelles par un contingent complet de capacités internes ne saurait rivaliser avec les savoir-faire de fournisseurs externes spécialisés qui tendent également à disposer de ressources plus abondantes à consacrer aux activités de développement et de recherche considérées comme indispensables dans le domaine dynamique de la cybersécurité. Il a également été fait valoir, cependant, que même lorsque des entités optent pour la solution de la sous-traitance, elles doivent s'assurer de la présence d'un niveau suffisant de capacités internes qui puissent assurer certains aspects des principales fonctions de la cybersécurité en ayant une connaissance approfondie du déroulement des activités et processus institutionnels, et également servir d'interface avec le fournisseur externe. Lorsque des centres des opérations de sécurité externes sont utilisés, la gestion du portefeuille des fournisseurs devient aussi une préoccupation majeure qui appelle une procédure d'agrément, des clauses de protection juridique adéquates dans les contrats et des précautions pour éviter la dépendance vis-à-vis d'un fournisseur donné. Certains des arguments pour ou contre l'acquisition d'un centre des opérations de sécurité en sous-traitance peuvent aussi valoir pour d'autres décisions relatives à l'utilisation de capacités internes ou externes de gestion de la cybersécurité ; ils sont résumés dans l'encadré 8.

Encadré 8

Arguments pour et contre le recours à des fournisseurs externes pour l'acquisition d'un centre des opérations de sécurité et d'autres services de cybersécurité

Arguments pour :

- Disponibilité de profils de compétences et d'outils variés, à jour et hautement spécialisés
- Éventuelle rationalisation de l'utilisation des ressources
- Possibilité d'accroître ou de réduire le niveau des services en fonction de l'évolution constante du paysage des menaces et de la fluctuation des capacités requises
- Perception de neutralité et d'impartialité

Contre :

- Risque de dépendance vis-à-vis d'un fournisseur donné (enfermement propriétaire)
- Éventuelles difficultés d'adaptation des services et des solutions standardisés conduisant à des solutions suboptimales et rigides
- Dépendance croissante vis-à-vis de personnels inconnus n'ayant pas fait l'objet des contrôles habituels et placés sous le contrôle direct de cadres
- Exposition potentielle de données sensibles à de tierces parties
- Transparence limitée dans le signalement des incidents
- Coûts

120. **Un centre des opérations de sécurité améliore la cohérence de la fonction de cybersécurité.** Chaque entité devrait évaluer l'opportunité de l'établissement d'un tel centre sur la base d'une analyse coûts-avantages au regard de paramètres tels que la complexité de la configuration de son infrastructure informatique et de communication, le nombre et le type d'actifs et de processus critiques gérés, le volume total des flux de données et, partant, la fréquence des menaces. Sur cette base seront établis, à différents degrés, les besoins en surveillance et protection constantes. Les Inspecteurs souhaitent attirer l'attention sur le fait qu'un des aspects les plus importants d'un centre officiel des opérations de sécurité − quelles que soient sa taille et ses capacités − tient à l'attention qu'il porte et la cohérence qu'il apporte à la surveillance et aux opérations quotidiennes de cybersécurité au sein d'une entité. Même s'il s'agit d'une très petite équipe qui doit compter sur des membres du personnel des services chargés des TIC situés ailleurs dans l'entité ou sur des fournisseurs externes, elle n'en est pas moins à même de jouer un rôle de coordination et de synchronisation et de sensibiliser l'entité. **Les Inspecteurs proposent par conséquent que les chefs de secrétariats envisagent la possibilité de créer un centre des opérations de sécurité ou de rationaliser les capacités existantes en un mécanisme équivalent sur la base d'un examen critique de leurs besoins institutionnels ainsi que des capacités internes et externes déjà à leur disposition, et qu'ils s'assurent d'être en mesure d'étayer pleinement toutes les raisons sur lesquelles repose leur décision favorable ou défavorable à la mise sur pied d'un centre des opérations de sécurité.**

K. Réflexion et communication sur les efforts d'amélioration de la cyberrésilience déployés à l'échelle de l'entité

121. La mesure dans laquelle les éléments exposés dans le présent chapitre se retrouvent dans la façon dont une entité aborde la question de sa cyberrésilience est en corrélation directe avec le dispositif et les capacités dont elle dispose pour cerner, prévenir et détecter les menaces, ainsi que pour riposter aux incidents et s'en remettre. En gardant à l'esprit le fait que les dispositions en place peuvent être le résultat de choix stratégiques ou opérationnels, ou qu'elles peuvent avoir été dictées par d'autres considérations, les chefs de secrétariat devraient entreprendre une étude à l'échelle de l'entité de la mesure dans laquelle chacun des éléments visés est intégré dans les politiques et les pratiques de leur entité.

122. L'application de la recommandation suivante devrait renforcer, dans le sens d'une plus grande efficacité, l'état de préparation et la capacité de riposte des entités des Nations Unies dans le domaine de la cybersécurité.

Recommandation 1

Les chefs de secrétariat des entités des Nations Unies devraient établir, à titre prioritaire et d'ici à la fin de 2022, un rapport exhaustif consacré à leur cadre de cybersécurité, qui aborde les facteurs d'amélioration de la cyberrésilience examinés dans le présent rapport, et présenter ce document, dans les meilleurs délais, à leurs organes délibérants et directeurs.

123. Les conclusions d'un tel examen interne, considérant les forces et les faiblesses relevées et proposant des mesures de renforcement de la cyberrésilience, devraient être communiquées aux organes délibérants et directeurs. De l'avis des Inspecteurs, ceux-ci seraient alors mieux à même de fournir des orientations stratégiques de haut niveau, sous la forme d'une déclaration explicite de l'appétit de l'entité pour le risque, et d'affecter des ressources à la réalisation du niveau de protection souhaité. Comme indiqué plus haut, la direction exécutive devrait envisager de rendre compte régulièrement des questions de cybersécurité aux organes délibérants et exécutifs. Les Inspecteurs sont conscients du caractère sensible que pourraient avoir certaines portions d'un tel rapport et de la nécessité, le cas échéant, de leur attribuer le niveau de confidentialité voulu. **Il est par conséquent conseillé à la direction exécutive de sélectionner avec le plus grand soin un format et une voie de communication qui permettent aux organes délibérants et directeurs de tirer le meilleur parti des informations fournies sans que ne soient compromises les défenses de l'entité.**

Recommandation 2

Les organes délibérants et directeurs des entités des Nations Unies devraient examiner les rapports établis par les chefs de secrétariat sur les facteurs d'amélioration de la cyberrésilience et fournir des orientations stratégiques concernant les améliorations qui doivent encore être apportées, le cas échéant, dans leurs entités.

IV. La cybersécurité à l'échelle du système

A. La cybersécurité : une priorité pour l'ensemble du système ?

124. **La collaboration au niveau du système en matière de cybersécurité : une priorité déclarée de longue date.** Le renforcement du dispositif de cybersécurité du système des Nations Unies est une priorité affirmée depuis de nombreuses années, tant par les États Membres que par les plus hauts responsables de l'ONU. En 2008, par exemple, l'Assemblée générale a incité le Secrétaire général, en sa qualité de Président du CCS, à susciter une intensification de la coordination et de la collaboration entre les organismes des Nations Unies sur toutes les questions relatives aux TIC, au progiciel de gestion intégré et, points importants, à la sécurité, à la reprise après sinistre et à la continuité des opérations[29]. En 2013, à l'issue de son examen d'un rapport sur l'état d'avancement de l'application des recommandations relatives au renforcement de la sécurité des systèmes informatiques du Secrétariat, le Comité consultatif sur les questions administratives et budgétaire a engagé le Secrétaire général à continuer de privilégier la coopération à l'échelle du système et de rechercher toutes les possibilités de coopération supplémentaire et de mutualisation des solutions de sécurité de l'information entre les organismes des Nations Unies[30]. Plus récemment, en 2019, en conclusion de délibérations tenues au niveau du CCS, le Secrétaire général lui-même a déclaré que le système des Nations Unies devait renforcer sa capacité de se protéger contre les cyberattaques[31]. L'hypothèse sous-jacente, à tous ces égards, est qu'une plus grande collaboration à l'échelle du système, notamment sous la forme de démarches communes et de solutions opérationnelles mutualisées, fait partie des facteurs clés conduisant à une meilleure protection du système dans son ensemble.

125. **Les tentatives d'adoption d'une démarche stratégique commune.** Comme on l'a vu, les entités des Nations Unies sont confrontées pour l'essentiel aux mêmes défis et menaces dans le cyberenvironnement. Ce qui devrait laisser entrevoir la possibilité de concevoir une approche commune en riposte. Étant donné que la sécurité du système dépend, du moins en partie, de la sécurité de ses membres pris individuellement, ceux-ci étant interconnectés à divers niveaux, il existe également une bonne raison de poursuivre cet objectif. Pendant la phase préparatoire du présent examen, plusieurs entités participantes ont plaidé en faveur de l'élaboration d'une stratégie commune qui leur appartiendrait, qu'elles suivraient et dont elles rendraient compte en tant que partenaires agissant de concert et mues par l'objectif commun d'atteindre entre elles un certain degré de maturité, sur la base d'une série de critères minima auxquels toutes devraient satisfaire. Une demande aux fins de la formulation d'une stratégie de cybersécurité globale, qui contribuerait à jeter les bases de pratiques de cybersécurité cohérentes dans tout le système, apparaît en 2017 dans les documents du Réseau Technologies de l'information et des communications[32]. Cette initiative ne semble toutefois pas avoir pris forme ou été poussée plus loin de quelque façon tangible que ce soit. Une autre tentative en faveur d'une approche harmonisée prévoyait notamment d'effectuer auprès des organisations des enquêtes annuelles concernant leurs mesures de cybersécurité de sorte à établir un indice interne de maturité, et de mieux évaluer ainsi l'exposition générale du système au risque. Malgré d'importants travaux préparatoires comprenant deux enquêtes pilotes menées auprès d'une vingtaine d'entités en 2018 et 2019, la proposition n'a pas recueilli à l'époque le soutien collectif nécessaire de la part des équipes de direction. Les principaux arguments avancés pour justifier le rejet de telles initiatives d'évaluation comparative étaient, d'une part, la diversité des configurations institutionnelles et des contextes en présence qui venait limiter la valeur d'une évaluation collective et, d'autre part, le peu d'engouement des entités à communiquer leurs évaluations internes en matière de cybersécurité, citant effectivement les cyberrisques comme étant le principal obstacle à la conduite ne fût-ce que d'une évaluation cumulative. Les avis recueillis dans le cadre des entretiens donnent à penser que la pandémie de COVID-19 pourrait avoir modifié les perceptions et les mentalités concernant la cybersécurité, et que des propositions

[29] Résolution 63/262 de l'Assemblée générale.
[30] A/68/7/Add.11, par. 6.
[31] CEB/2019/2, par. 39.
[32] CEB/2017/HLCM/ICT/9, p. 7 et 8 (en anglais)

précédemment considérées comme trop ambitieuses ou peu réalistes pourraient aujourd'hui avoir plus de chances de susciter un intérêt et d'être favorablement accueillies. En fait, un débat portant sur la possibilité d'appliquer un modèle de maturité de référence similaire à celui récemment adopté par le Forum de gestion des risques du CCS semble avoir refait surface dans le cadre de la dernière réunion interentités des spécialistes de la cybersécurité.

126. **Une responsabilité collective pour garantir un niveau de défense minimum.** Une harmonisation totale au niveau du système tout entier, à plus forte raison si elle est fondée sur une évaluation comparative des niveaux de maturité des entités, peut effectivement s'avérer par trop ambitieuse, et même hors de propos. Comme l'a déclaré le centre de réflexion Gartner, si la tentative de comparer entre eux les systèmes et mesures de cybersécurité des entités en présence peut amener à constater leur maturité relative, mais ne donne pour aucune d'entre elles d'indication fiable du degré de protection absolu[33]. En revanche, leur interdépendance sur le plan de la réputation et des opérations crée entre elles une responsabilité collective qui les engage toutes à viser le plus haut niveau possible de cybersécurité et à s'entraider à cette fin. À noter que ce sont les entités dotées d'un cadre de cybersécurité avancé et de solides capacités internes ou externes qui ont montré le plus d'engouement pour des efforts dans ce sens. L'exercice est délicat, mais il est crucial que le système trouve le juste équilibre entre les exigences propres aux entités participantes, leurs dispositifs existants et une démarche systémique qui permette d'établir une norme minima à satisfaire par toutes pour le bien de toutes. **De l'avis des Inspecteurs, la définition du niveau de protection de base ainsi que des exigences de défense minima applicables aux entités des Nations Unies, et par conséquent au système tout entier, reste un objectif valable qui mérite d'être poursuivi**.

127. **Les efforts déployés pour instaurer des capacités partagées au niveau opérationnel.** L'opportunité d'instaurer, à l'échelle du système, des capacités fédérées qui servent à prendre des mesures de prévention, de détection et de riposte contre les menaces à la cybersécurité et les cyberattaques est une question qui a été débattue plusieurs fois à divers niveaux. Il y a bientôt dix ans, le Réseau Technologies de l'information et de la communication a produit une feuille de route pour l'établissement d'une équipe d'intervention des Nations Unies en cas d'atteinte à la sécurité de l'information[34]. Il n'a pas été donné suite à cette initiative faute d'accord sur le mode de financement à l'époque. Plus récemment, le Groupe d'intérêt pour la sécurité informatique a repris son étude de la faisabilité d'un centre des opérations de sécurité qui serait commun aux entités des Nations Unies. La discussion parmi ses membres a mis en évidence une quantité de questions pendantes (partage des frais, alignement sur diverses configurations existantes, accord sur la portée et les priorités des interventions en cas d'attaque généralisée, etc.). Ces tentatives partaient du principe que la mise sur pied de capacités d'intervention à l'échelle du système pourrait donner lieu à d'importants gains d'efficience tout en offrant une protection accrue, en particulier aux entités qui n'avaient pas les moyens de s'équiper de capacités de réserve au cas où une attaque toucherait au but. Il ressort toutefois de ces tentatives que les objectifs visés, quoique clairs et largement soutenus, sont plus difficiles à mettre en pratique que l'on ne pourrait s'y attendre. L'expérience montre que dès qu'un pas est franchi vers leur concrétisation, leur mise en œuvre se fait plus insaisissable.

128. **L'accueil mitigé réservé à la formation et à la sensibilisation en tant que candidates à la mise en commun de ressources à l'échelle du système.** La formation et la sensibilisation à la cybersécurité avaient fait l'objet d'une proposition prometteuse mais, à plus ample examen, l'accueil qui leur a été réservé est apparu mitigé. La question de la collaboration relative aux programmes d'apprentissage dans le système des Nations Unies a été examinée dans un récent rapport du CCI[35]. Un des constats du rapport portait sur le double emploi des efforts consacrés à la création de programmes similaires par différentes entités. De prime abord, le domaine de la formation et de la sensibilisation à la cybersécurité semblaient prédestinés à la collaboration à l'échelle du système et à la mutualisation des ressources. En partant du principe que l'essentiel de la formation des utilisateurs finals

[33] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, février 2020.

[34] CEB/2013/5, par. 38 et 39 (en anglais).

[35] JIU/REP/2020/2.

pouvait être standardisé, dès lors qu'une grande part du matériel d'apprentissage ne devait pas être spécifique à une entité, le paysage des menaces étant partagé, un des premiers projets conjoints réalisés par le Groupe d'intérêt pour la sécurité informatique a consisté à produire les modules de base d'un programme d'apprentissage commun portant sur la cybersécurité, à charge pour les membres du Groupe de les utiliser ensuite moyennant adaptation. La démarche du programme d'apprentissage semble avoir suscité un certain intérêt de la part de plusieurs entités qui ont choisi d'adopter le module de formation en ligne à la sécurité de l'information du Secrétariat de l'ONU ou qui ont fait appel au CIC et à son service de sensibilisation à la sécurité de l'information pour adapter les contenus concernés. Il n'a toutefois pas été donné aux Inspecteurs de constater un consensus marqué parmi les entités participantes sur les avantages d'une mise en commun de la formation. En réalité, plusieurs entités ont plaidé avec vigueur contre une approche standardisée, arguant notamment de la spécificité des mandats des unes et des autres, des contraintes imposées par un processus commun d'élaboration qui, par ses fréquentes lenteurs, rendait rapidement obsolètes les contenus conçus en commun, et n'était pas facile à remplacer, alors que ses produits tendaient nécessairement vers un « plus petit commun dénominateur » qui risquait de ne pas répondre aux attentes des utilisateurs sans que ne soient encore consentis de considérables investissements pour les adapter et les étoffer. Au vu de ces considérations, un certain nombre d'entités ont mis au point leurs propres modules de formation, parfois en coopération avec des fournisseurs externes, à un coût non négligeable. **Les Inspecteurs restent convaincus que les entités des Nations Unies tireraient avantage d'une certaine harmonisation des formations, même si celles-ci doivent ensuite être adaptées aux besoins de certaines d'entre elles.**

129. **L'optimisation des ressources destinées à la cybersécurité.** Tous les spécialistes et cadres interrogés convenaient que les entités des Nations Unies, considérées individuellement ou collectivement, étaient d'envergure modeste comparées à celles du secteur privé, et que les ressources dont elles disposaient pour faire face et riposter aux attaques externes plus sophistiquées émanant de la criminalité organisée, ou d'autres attaques parrainées, étaient au mieux limitées. Cela étant, il n'est pas rare que les entités consacrent des ressources à la cybersécurité de façon isolée et pour leurs propres besoins, parfois parce qu'elles doivent réagir sous la pression d'un fait particulier. Il y a un net sentiment au sein du système que des gains d'efficience peuvent être réalisés en adoptant une approche conjointe de la cybersécurité. Cela étant, le tableau dressé par les réponses des entités participantes du CCI concernant des domaines où la mutualisation des ressources pourrait être envisageable et utile présentait des divergences. Un domaine qui a recueilli des avis favorables quant à la possibilité d'y réaliser des économies est le recours aux prestataires de services du secteur commercial et privé. De nombreuses entités ont dit utiliser de tels services, citant souvent les mêmes prestataires pour des services identiques ou similaires, tels que l'évaluation des risques et des vulnérabilités, les audits relatifs à la norme ISO 27001 et les solutions logicielles, ce qui signifie que chacune avait soumis ces entreprises à ses propres procédures d'agrément et de gestion des fournisseurs, et les avait aussi payées séparément. Seules une poignée d'entités ont dit avoir bénéficié de mémorandums d'accord ou de dispositions similaires conclues entre elles pour tirer mutuellement parti de leurs processus de passation des marchés ou de leurs contrats de services relatifs aux protections et ripostes relevant de la cybersécurité, et ce, en dépit de l'existence d'un accord de reconnaissance mutuelle signé par 20 entités. Si les Inspecteurs reconnaissent l'existence de facteurs qui limitent la mise en œuvre de telles initiatives conjointes, ils n'en estiment pas moins que ces initiatives méritent plus d'attention en ce qu'elles pourraient permettre des gains d'efficacité. Un certain nombre d'obstacles aux achats conjoints ou concertés en général ont été relevés par les Inspecteurs dans le cadre des entretiens et des questionnaires. Les différentes procédures et règles de passation des marchés qui se côtoient dans le système sont des barrières qui viennent limiter les achats concertés. Certains obstacles ne sont toutefois pas directement liés aux règles et procédures, mais plutôt à la culture qui préside au fonctionnement d'une entité et qui peut proscrire la coopération libre en faveur d'un contrôle institutionnel strict. Certaines de ces barrières tiennent à des différences de logique opérationnelle entre une gestion hautement centralisée des achats et une passation des marchés décentralisée, à des différences entre modalités de financement (dans le cas des paiements anticipés, par exemple) et à un manque d'uniformité pami les systèmes informatiques et les systèmes de comptes fournisseurs, comme en rend compte un rapport du

CCI consacré aux achats[36]. S'il s'avère que l'achat conjoint de certains services n'est pas possible, les entités participantes devraient à tout le moins faire tout ce qui est en leur pouvoir pour coordonner autant que possible leurs achats. Autrement, elles courent le risque de voir les prestataires commerciaux tirer parti de ces pratiques d'achats incohérentes pour facturer leurs services à des prix différents au sein du système et créer, ce faisant, une sorte de concurrence dont ils seront les seuls à profiter, au détriment des intérêts financiers des entités concernées.

130. **L'absence d'efforts véritablement concertés à l'échelle du système au-delà de mesures de coordination et de solutions opérationnelles partielles.** On peut dire que l'importance acquise et la dynamique créée par la cybersécurité aux plus hauts niveaux sont telles qu'elles ont créé les conditions optimales pour donner une puissante impulsion à l'établissement de capacités à l'échelle du système. Cependant, en dépit de la disponibilité de plusieurs ressources, mécanismes et initiatives d'importance au sein du système, de même qu'une volonté politique apparente dans ce sens, les signes que ces déclarations ambitieuses se feraient réalité sont loin d'être évidents. À ce stade, le système ne dispose pas d'une entité qui soit officiellement chargée de mener le programme d'harmonisation de la cybersécurité, ni de concevoir et d'appliquer des solutions partagées pour les entités des Nations Unies. Les efforts déployés à l'échelle du système en matière de cybersécurité sont institutionnellement concentrés autour de mécanismes de coordination interentités relevant du CCS, et ils reçoivent un certain appui, sur le plan opérationnel, du CIC, qui fournit certains services partagés à plusieurs entités des Nations Unies. Dans le présent chapitre, les Inspecteurs examinent les arrangements institutionnels et opérationnels en place, y compris le décalage qui semble exister entre eux et les tendances interentités dominantes en la matière (annexe VI). Ils s'attachent également à déterminer les progrès réalisés à ce jour, les avantages et les contraintes inhérents à la situation actuelle, ainsi que les domaines qui pourraient se prêter à une action collective renforcée en vue de l'élaboration de ripostes au niveau du système des Nations Unies dans son ensemble, dans la mesure de ce qui est pratique et raisonnable.

B. Les mécanismes interentités ayant trait à la cybersécurité

131. **Un intérêt de longue date de la part des mécanismes interentités.** Sous l'appellation « sécurité des systèmes d'information », la cybersécurité figure dans le discours de l'informatique au niveau du système depuis l'époque du Comité consultatif pour la coordination des systèmes d'information. Dès 1994, un groupe de travail établi par le prédécesseur du Réseau Technologies de l'information et des communications (devenu Réseau Technologie et numérique en 2018) a été chargé d'examiner une série de directives relatives à la sécurité des systèmes d'information pour les entités des Nations Unies, publiées en 1992[37]. Il y a donc fort à croire que la question avait déjà fait l'objet d'une attention considérable avant cela. À noter que les directives représentent un travail exhaustif et étonnement progressiste de relevé et d'orientation portant sur les multiples dimensions de la cybersécurité, à la fois au niveau de l'encadrement et des opérations, dont la terminologie quelque peu ancienne ne doit pas occulter le fait qu'une part non négligeable de son contenu et de ses recommandations restent valables même après une trentaine d'années.

132. **Un intérêt de longue haleine pour une démarche coordonnée en matière de cybersécurité.** L'idée d'une riposte coordonnée aux menaces à la cybersécurité figurait toujours dans les documents officiels dix ans plus tard, en 2002, lorsque les membres du CCS ont reconnu que, même lorsque les besoins en sécurité des entités se rangeaient dans des catégories différentes (certaines abritant des bases de données extrêmement confidentielles et sensibles), d'importantes questions communes à toutes devaient être prises en considération de toute urgence[38]. En 2010, il semble que la notion de « sécurité des systèmes informatiques » ait été supplantée par celle de « cybersécurité », dont l'usage a connu un élan

[36] Voir JIU/REP/2013/1.

[37] Comité consultatif pour la coordination des systèmes d'information, *Information System Security Guidelines for the United Nations Organizations*, New York, 1992.

[38] CEB/2002/HLCM/10, par. 8 (en anglais).

considérable avec la proposition renouvelée, face aux « menaces croissantes pesant sur la cybersécurité » et au « cybertsunami » que représentaient leurs effets dévastateurs potentiels dans « tous les secteurs », d'une « matrice pour traiter le problème à l'échelle du système »[39]. Des déclarations similaires ont été faites au cours des années qui ont suivi, dans le cadre du Comité de haut niveau sur la gestion, concernant le terrain d'entente considérable qui existait quant à la meilleure manière de protéger les entités des Nations Unies contre la perturbation de leurs activités et les menaces à leur sécurité[40], et dans le cadre du Réseau Technologies de l'information et des communications, concernant « le renforcement de la capacité de nos institutions à résister aux attaques informatiques » qui devait « demeurer une priorité »[41].

133. **Les documents marquants relatifs à la cybersécurité et à la cybercriminalité adoptés à l'échelle du système en 2013 et 2014.** En 2010, le CCS a chargé le Comité de haut niveau sur la gestion et le Comité de haut niveau sur les programmes de se saisir ensemble de la question, sous la direction de l'UIT et de l'Office des Nations Unies contre la drogue et le crime (ONUDC), auxquels se sont joints par la suite la Conférence des Nations Unies sur le commerce et le développement (CNUCED), le PNUD et l'UNESCO. Cette initiative transversale a trouvé son point culminant avec l'approbation du cadre à l'échelle du système des Nations Unies sur la cybersécurité et la cybercriminalité en 2013[42] et, en prolongement de ce cadre, le plan de coordination interne du système des Nations Unies sur la cybersécurité et la cybercriminalité en 2014[43]. Bien que les deux documents portent principalement sur la dimension « externe » du travail des Nations Unies (c'est-à-dire les activités programmatiques conçues pour soutenir les États Membres dans leurs activités en la matière), ils fournissent un solide point de départ pour établir les grandes orientations de la dimension « interne » de la cybersécurité pour le système (encadré 9). Les Inspecteurs ont cependant remarqué qu'aucune des entités participantes n'avait mentionné ce cadre ou ce plan lors de la préparation du présent examen. Bien que le plan ne semble pas être devenu une référence durable pour le système, les Inspecteurs ont été rassurés par le fait que les principes et les éléments fondamentaux qu'il contenait continuaient d'éclairer les plans de travail des organes interentités concernés.

Encadré 9
Cadre et plan de coordination interne du système des Nations Unies sur la cybersécurité et la cybercriminalité

Approuvé par le CCS à sa deuxième session ordinaire en 2013, le cadre à l'échelle du système des Nations Unies sur la cybersécurité et la cybercriminalité jette les bases d'une action coordonnée des entités des Nations Unies en réponse aux préoccupations des États Membres dans ces domaines.

Le cadre :

- Fournit la définition commune de certains concepts clés et trace les contours de la matière ;
- Met en évidence les zones d'intersection entre les mandats pertinents des entités concernées ;
- Établit les principes de base de la conception de programmes et de l'assistance technique dans les domaines de la cybercriminalité et la cybersécurité ;
- Contient des orientations pour que la fourniture d'assistance technique aux États Membres donne lieu à une coopération renforcée dans ces domaines.

[39] CEB/2010/1, par. 53.
[40] CEB/2013/5, par. 36 (en anglais).
[41] CEB/2013/2, par. 58.
[42] Ibid., par. 85, et annexe III (Cadre à l'échelle du système des Nations Unies sur la cybersécurité et la cybercriminalité).
[43] *United Nations system internal coordination plan on cybersecurity and cybercrime*, novembre 2014 (document interne).

Conçu en 2014, en prolongement de ce cadre, pour guider la coordination interne parmi les entités des Nations Unies dans les domaines de la cybersécurité et de la cybercriminalité, le plan de coordination interne du système des Nations Unies sur la cybersécurité et la cybercriminalité s'articulait autour de cinq thèmes relevés par le Secrétaire général comme se prêtant à des actions communes au sein du système. Pour chaque thème, le plan énonçait un éventail de principes et de points d'action que les entités étaient invitées à adopter. Les chefs de secrétariat étaient particulièrement encouragés à lancer un cours informatisé obligatoire de formation du personnel à la cybersécurité, fondé sur le programme de formation convenu par le Réseau Technologies de l'information et des communications, et à mettre sur pied une équipe interentités d'intervention en cas d'atteinte à la sécurité de l'information. Ces deux derniers points d'action sont aussi ceux qui ont été jugés pertinents pour le Comité de haut niveau sur la gestion, par le Président de celui-ci (CEB/2014/5, par. 72).

Le thème suivant intéresse tout particulièrement le présent examen :

Thème 1 : Veiller à la préparation interne nécessaire pour faire face aux menaces à la cybersécurité, au niveau des entités individuelles et à l'échelle du système des Nations Unies, en incluant les obstacles liés aux politiques et aux ressources qui peuvent empêcher les entités d'agir de concert pour assurer une meilleure protection commune du système des Nations Unies, en recourant, par exemple, à l'intégration de la cybersécurité dans les cadres d'évaluation et de gestion des risques.

134. **Le Groupe d'intérêt pour la sécurité informatique en tant que principale plateforme spécialisée consacrée à la cybersécurité.** Dans l'ensemble, il a été établi que la structure chargée de la cybersécurité au niveau du système des Nations Unies existait de longue date et qu'en général, elle fonctionnait. Le Groupe d'intérêt pour la sécurité informatique, créé en 2011 en tant que principal mécanisme du système des Nations Unies chargé de promouvoir la coopération et la collaboration interentités dans le but d'optimiser la sécurité de l'information, est rattaché au Réseau Technologies de l'information et des communications, dont il reçoit des instructions, et fonctionne sous la supervision générale du Comité de haut niveau sur la gestion. Conformément à son mandat, sa composition est explicitement limitée aux responsables de la sécurité de l'information, ou équivalents, des entités membres du CCS. Lorsque cette fonction n'existe pas, c'est habituellement un fonctionnaire des services informatiques et de communication qui représente l'entité concernée. Les modalités de travail du Groupe d'intérêt comprennent un symposium annuel auquel prennent part des orateurs externes, une session exécutive tenue lors du symposium, à laquelle sont prises des décisions formelles, et des groupes de travail à durée limitée dans le cadre desquels les entités chef de file se portent volontaires pour mener des délibérations sur des sujets d'intérêt particulier. Plusieurs entités qui ne sont pas membres du CCS, dont le CIC, prennent part aux travaux du Groupe d'intérêt en qualité d'observateurs, sans droit de vote. Le Groupe d'intérêt est présidé, à tour de rôle, par un de ses membres officiels. Au moment de rédiger le présent rapport, ce rôle était assuré par le Bureau de l'informatique et des communications du Secrétariat de l'ONU.

135. **L'utilité confirmée du principal organe interentités en tant que plateforme d'échange.** Le Groupe d'intérêt pour la sécurité informatique a acquis une crédibilité professionnelle considérable en tant que plateforme officielle qui permet aux praticiens de la cybersécurité du système des Nations Unies de se retrouver régulièrement et de se pencher sur les difficultés, les perspectives et les bonnes pratiques relatives au système dans son ensemble. Il ressort de l'analyse de rapports récents du Groupe d'intérêt qu'une variété de questions opérationnelles et stratégiques y font l'objet de riches débats et d'un grand intérêt. Il y est notamment question de la sécurité et de la gestion des risques de l'informatique en *cloud* (ou en nuage), de la gestion des identités numériques, de l'évaluation comparative de la maturité en matière de cybersécurité, de la formation de sensibilisation à la sécurité de l'information et, plus récemment, de l'idée d'un centre des opérations de sécurité partagé ainsi que du regroupement des services de renseignement sur les menaces. Dans leurs réponses au questionnaire du CCI, les deux tiers environ des entités participantes ont d'ailleurs dit voir dans le Groupe d'intérêt un moyen efficace de promouvoir la coopération et la collaboration entre les entités des Nations Unies, et apprécier les contributions

fonctionnelles de ses membres ainsi que les possibilités d'échanges avec des spécialistes externes, y compris du secteur privé. Nombreux sont les membres qui ont loué les efforts déployés par le Président pour faciliter le débat et faire progresser l'exécution du plan de travail du Groupe d'intérêt. Certains aspects plus faibles du fonctionnement du Groupe d'intérêt sont déjà pris en main, tels que la faible fréquence de ses symposiums et le peu d'interaction dans l'intervalle entre les sessions, occasions que certains membres voudraient voir étoffer pour faciliter un dialogue plus continu et moins formel. En réponse à un besoin évident à cet égard, un canal spécial de messagerie instantanée a été mis sur pied pour permettre aux membres du Groupe d'intérêt d'avoir des échanges directs et informels, notamment lorsqu'il est nécessaire de communiquer rapidement ou de partager des informations. Les efforts déployés en faveur d'échanges plus quotidiens ont fait l'objet de mentions favorables de la part des responsables de la sécurité de l'information, qui ont également confirmé avoir été des utilisateurs actifs de tels canaux dans le cadre de leurs tâches quotidiennes.

136. **Les structures interentités sont saisies de la question de la cybersécurité à tous les niveaux.** Depuis le Groupe d'intérêt pour la sécurité informatique jusqu'au Réseau Technologie et numérique et au Comité de haut niveau sur la gestion, il s'avère que la cybersécurité est activement débattue et reconnue comme une question d'importance critique. La sécurité de l'information et la cybersécurité figurent parmi les 10 objectifs énoncés dans le mandat, révisé en 2019, du Réseau Technologie et numérique qui réunit les responsables des services informatiques du système et reçoit les rapports et recommandations du Groupe d'intérêt pour la sécurité informatique pour approbation et transmission au Comité de haut niveau pour la gestion[44]. Dans la pratique et dans l'ensemble, on peut dire que le Réseau a accueilli favorablement les travaux du Groupe d'intérêt pour la sécurité informatique, étant donné qu'il ne s'est écarté des positions adoptées par celui-ci que dans une poignée de cas, et qu'il a en outre approuvé la majorité de ses recommandations, parfois moyennant modifications. Au niveau du Comité de haut niveau sur la gestion, qui a joué un rôle important dans l'élaboration du cadre de 2013 et du plan de coordination de 2014, la cybersécurité fait partie des plans stratégiques, y compris du plus récent pour la période 2017-2020, en tant qu'élément de la priorité stratégique que constituent la gestion des risques et le renforcement de la résilience. Le dernier plan contient une déclaration selon laquelle le Comité de haut niveau redoublera d'efforts pour promouvoir la mise en œuvre à l'échelle du système de mesures de surveillance et de riposte, y compris d'atténuation, face aux menaces à la cybersécurité[45]. Il ressort toutefois de la documentation officielle du Comité de haut niveau que si la cybersécurité y figure en tant que préoccupation d'ordre général, il est rare que des recommandations et des éléments spécifiques en la matière atteignent ce niveau. Les Inspecteurs relèvent à cet égard que dans leur réponse au questionnaire du CCI, un tiers seulement des entités participantes ont déclaré considérer le Groupe d'intérêt pour la sécurité informatique comme un moyen efficace d'inciter à l'action aux échelons supérieurs de la structure du CCS.

137. **La mise en application des conseils et orientations émanant du Groupe d'intérêt pour la sécurité informatique dépend de ses membres.** Au cours du présent examen, les Inspecteurs ont constaté que la coordination et la coopération interentités en matière de cybersécurité au sein du système des Nations Unies devait encore livrer les résultats attendus. Bien que le travail conceptuel avance d'année en année dans le cadre des activités du Groupe d'intérêt pour la sécurité informatique, et que la question mobilise l'attention des équipes de direction, les solutions partagées, les approches communes ou concertées, et les projets conjoints ont été lents à se matérialiser. À titre de contexte, il est utile de se rappeler que la mouture actuelle du mandat du Groupe d'intérêt, dont la dernière révision date de 2018[46], confirme sa vocation de partage des connaissances, des expériences et des solutions, et inclut notamment la réalisation de projets communs. Plus tard au cours de la même année, lorsque le Réseau Technologies de l'information et des communications est devenu le Réseau Technologie et numérique, et que le mandat de chacun de ses sous-groupes a été revu, le Réseau est allé encore plus loin, décidant qu'outre la poursuite de ses activités tendant à

[44] CEB/2019/HLCM/DTN/03/R1, p. 2 (en anglais).
[45] CEB/2016/HLCM/15, p. 13 (en anglais).
[46] CEB/2018/HLCM/ICT/3/Rev.1 (en anglais).

promouvoir la collaboration et le partage des connaissances parmi les entités, le Groupe d'intérêt pour la sécurité informatique devait prendre une part plus active dans la conception et la diffusion de solutions partagées et d'innovations[47]. Ce projet du Réseau de voir son sous-groupe s'impliquer de façon plus pratique dans la conception de solutions pour le système n'a, semble-t-il, donné lieu à aucune mobilisation de capacités opérationnelles indépendantes des ressources internes et des engagements individuels de ses membres. Le Groupe d'intérêt manque de facto d'un mécanisme efficace pour faciliter la concrétisation et la mise en place communes des solutions conçues ou des accords conclus dans le contexte interentités. Considérant qu'il n'est pas du ressort principal d'un organe de coordination de s'occuper de l'application de ses propres recommandations, le fait que le système ne dispose pas d'une « composante opérationnelle » officiellement approuvée, qui prenne ses ordres du collectif des responsables de la sécurité de l'information et soit au service de l'intérêt commun, compte parmi les principaux facteurs qui, de l'avis des Inspecteurs, font obstacle à ce que la cybersécurité trouve une véritable dimension systémique. La question de savoir si des mécanismes ou des organes existants peuvent raisonnablement combler cette lacune est examinée plus en détail dans les sections suivantes du présent rapport.

138. **Le renforcement du pouvoir d'action individuel et collectif des responsables de la sécurité de l'information.** À l'examen, le profil des membres du Groupe d'intérêt pour la sécurité informatique s'est avéré inégal, allant du niveau opérationnel au niveau stratégique, certains responsables occupant des postes à la classe de début de la catégorie des administrateurs, tandis que d'autres exerçaient des fonctions de cadres de rang intermédiaire à supérieur, voire de direction de départements entiers. Au-delà du niveau de connaissances spécialisées et de la culture de franche discussion qui caractérise le Groupe d'intérêt, selon ses membres, l'hétérogénéité de sa composition affecterait sa dynamique et aurait des effets directs sur sa capacité de formuler à l'intention du système des orientations faisant autorité. Chaque membre ayant des moyens d'action différents au sein de la structure de sa propre entité, avec ce que cela impose comme limites à sa capacité de prendre des engagements au nom de celle-ci dans le cadre des initiatives interentités, les occasions données au Groupe d'intérêt de jouer un rôle transformateur, tant au niveau des entités que collectivement, par une action concertée au niveau du système, sont limitées. En tant qu'organe de coordination, le Groupe d'intérêt fait face aux mêmes difficultés à cet égard que tout autre mécanisme interentités dépourvu du pouvoir décisionnel nécessaire pour imposer des mesures au niveau du système. C'est pourquoi il ne serait pas réaliste de s'attendre à ce qu'il constitue un cadre de mise en œuvre. De même qu'il n'a que peu d'influence sur la façon dont les résultats de ses travaux sont répercutés aux équipes dirigeantes de chaque entité. Les documents officiels du Réseau Technologie et numérique font clairement ressortir que ces limites sont bien comprises, comme attesté par le fait que le Réseau ait appelé ses propres membres − les responsables des services informatiques − à autonomiser leurs responsables de la sécurité de l'information, entre autres, en leur délégant des pouvoirs supplémentaires[48]. On se rappellera aussi que le Groupe d'intérêt lui-même est placé sous l'autorité du Réseau Technologie et numérique, ce qui reproduit l'organisation et les difficultés associées constatées dans la plupart des entités, à savoir que le responsable de la sécurité de l'information est placé sous l'autorité du responsable du service des TIC. Pour pallier les effets contraignants de l'agencement actuel, **les Inspecteurs répètent leur appel à l'octroi de moyens d'action internes supplémentaires aux responsables de la sécurité de l'information, y compris, lorsque ce poste existe, en lui reconnaissant une fonction d'encadrement et en le rendant indépendant de la gestion des TIC dans la mesure du possible, et lorsque ce poste n'existe pas, en veillant à sa création.** En ce qui concerne les moyens d'action des responsables de la sécurité de l'information en tant que groupe, les Inspecteurs ont constaté qu'il y avait généralement peu d'engouement pour la promotion du Groupe d'intérêt dans les mécanismes interentités moyennant son découplage d'avec le Réseau et son accession au statut de réseau, ce qui lui permettrait de rendre compte directement au Comité de haut niveau sur la gestion. D'une part, les arguments contre ce remaniement incluaient la prolifération générale des réseaux, équipes spéciales et autres plateformes de coordination au sein de l'appareil du CCS, considérée comme peu susceptible, en soi, de contribuer à promouvoir la

[47] CEB/2018/HLCM/ICTN/18, p. 6 (en anglais).

[48] Voir, par exemple, CEB/2017/HLCM/ICT/9, p. 8 (en anglais).

question ou à lui conférer un degré de priorité effectivement plus élevé. D'autre part, l'opinion dominante semblait être que le Groupe d'intérêt disposait déjà, par l'entremise du Réseau Technologie et numérique et du Comité de haut niveau sur la gestion du solide canal dont il avait besoin pour mettre la question de la cybersécurité au premier plan des discussions stratégiques à l'échelle du système. **Les Inspecteurs ont réaffirmé que le Groupe d'intérêt pour la sécurité de l'information avait effectivement amélioré la mise en commun des informations relatives à la cybersécurité au sein du système des Nations Unies et qu'il devrait continuer de jouer ce rôle sans qu'il faille modifier l'architecture dans laquelle il s'inscrivait. Les Inspecteurs n'en soulignent pas moins la nécessité de concevoir un mécanisme qui permette au Groupe d'intérêt pour la sécurité informatique − en tant qu'entité distincte − de fournir des orientations stratégiques de la part du CCS et du système des Nations Unies.**

C. Les services de cybersécurité du Centre international de calcul des Nations Unies

139. **L'opportunité de revoir le potentiel non réalisé du CIC.** Dans le cadre de son rapport de 2019 sur l'informatique en *cloud* (ou en nuage), le CCI a déjà été appelé à examiner plus avant les conditions d'une mise en valeur, au bénéfice du système des Nations Unies, du potentiel non exploité du CIC et de sa gamme variée de services informatiques. À l'époque, la cybersécurité était considérée comme un des domaines où ce potentiel méritait que l'on s'y intéresse de plus près. Cela étant, compte tenu des perspectives ouvertes par la réforme des activités d'appui au sein de l'ONU, les Inspecteurs conviennent qu'il est opportun d'entreprendre une étude distincte, plus globale, du CIC et de son fonctionnement général, de son modèle d'activité, de sa structure de gouvernance et de son mandat, en allant même au-delà, éventuellement, de son rôle établi de prestataire de services informatiques. Depuis la création du CIC en 1971, faisant suite à la présentation à l'Assemblée générale d'un rapport d'audit externe détaillé commandé par le Secrétaire général, en sa qualité de Président du mécanisme de coordination concerné, pour étudier les installations et les besoins de l'ONU, de ses institutions spécialisées et de l'AIEA en matière de traitement des données[49], le Centre n'a fait l'objet d'aucun examen pour suivre son évolution et analyser de façon critique ses capacités et son potentiel inhérent de répondre aux besoins plus contemporains du système. Prenant acte des appels précédents du CCI pour que soient relevés d'éventuels obstacles à cet égard, et sans préjudice de l'application des recommandations formelles contenues dans le présent rapport, **les Inspecteurs considèrent qu'une analyse exhaustive du CIC pourrait être entreprise à l'avenir, en particulier afin de déterminer les conditions structurelles, financières et administratives qui lui permettraient de réaliser tout son potentiel en tant que partenaire et ressource stratégique pour l'ensemble du système des Nations Unies dans son ensemble.** Dans le cadre du présent rapport, une des questions qui a guidé les Inspecteurs dans leur examen de l'offre de services du CIC en matière de cybersécurité plus particulièrement, de son organisation et de la façon dont il envisageait son propre positionnement dans ce domaine précis, était celle de savoir si et dans quelle mesure les conditions étaient déjà réunies pour que le Centre devienne une plaque tournante de la cybersécurité au sein du système des Nations Unies.

Mandat et modèle d'activité

140. **L'évolution du CIC de 1971 à 2021.** Conformément à la résolution 2741 (XXV) de l'Assemblée générale, le CIC a été créé par mémorandum d'accord conclu en 1971 entre l'ONU, le PNUD et l'OMS. En tant que dispositif interentités initialement mis sur pied pour fournir des services de traitement électronique des données à ses trois membres fondateurs et d'autres utilisateurs, son catalogue et sa clientèle ont considérablement évolué depuis les années 1970. Mieux connu pour ses services d'hébergement et l'infrastructure informatique et de communication partagée qu'il met à la disposition des progiciels de gestion intégrés de bon nombre de ses clients, le CIC a vu son champ d'activité s'étendre dans des domaines aussi variés que l'informatique en *cloud* (ou en nuage), l'automatisation robotisée des

[49] A/8072 (en anglais).

processus, la chaîne de blocs, la conception de logiciels, les conseils en matière de TIC, et la cybersécurité. Sa clientèle a connu une croissance tout aussi considérable. Conçu dès le départ pour répondre aux besoins d'autres entités des Nations Unies que ses trois membres fondateurs, il en servait plus de 25 en 2003 et comptait quelque 70 clients en 2021, parmi lesquels, outre des entités des Nations Unies, des organisations affiliées, des organisations non gouvernementales (ONG) internationales et des institutions financières internationales. Son instrument constitutif a été modifié en 2003, afin d'élargir son assise juridique et de préciser les règles d'engagement relatives à son fonctionnement, par l'adjonction d'un document de « mandat » nouvellement formulé qui concrétisait et étendait les quelques dispositions de base contenues dans le document originel. Le nouveau texte, adopté séparément par toutes les entités partenaires dans le cadre du comité de gestion du CIC, exposait la structure de gouvernance du Centre, son modèle d'activité et les conditions fondamentales de participation. Les deux fonctions principales du CIC, telles que les présente ce document, sont de fournir des services informatiques, y compris des services opérationnels et des formations, et de s'employer à ce que la gamme des services offerts reflète les besoins des entités partenaires.

141. **Les grands principes du mandat et du modèle d'activité du CIC.** La mise à jour du mandat du CIC est venue renforcer l'objet originel de sa création en tant que prestataire de services aux entités des Nations Unies, liant étroitement son offre de services aux demandes concrètes générées par ses clients. La reformulation de ses principales fonctions lui a par ailleurs permis de se montrer aussi volontaire que possible dans sa recherche de nouvelles lignes de services, hors le cadre restreint du traitement des données, ce qui lui a notamment donné la liberté de proposer des services de cybersécurité sans qu'il n'y soit fait expressément référence dans son mandat. Un élément qui a été remis en évidence et développé dans le nouveau document est le concept d'infrastructure et de services partagés, dont le but est de réaliser des économies d'échelle au bénéfice des clients du Centre. Il s'agit de son modèle dit de services partagés, qui lui permet de réduire le coût de ses prestations en proportion directe de l'augmentation du nombre de clients qui s'abonnent à tel ou tel service. À côté de cela, certains éléments sont restés inchangés pendant les cinquante années d'existence du CIC. Ils comprennent : a) son modèle de récupération des coûts qui exige effectivement que tous ses produits soient préfinancés par les clients sur la base de besoins établis et moyennent l'approbation commune, sans qu'aucun surplus financier ni marge budgétaire ne puissent être générés en faveur d'activités de recherche-développement ; b) la nature facultative de son catalogue de services, auquel les entités peuvent recourir contre rémunération, ou auquel elles peuvent préférer la formule du service optionnel ; c) sa dépendance vis-à-vis d'une « organisation hôte » (l'OMS en l'occurrence), à laquelle il reste administrativement et juridiquement rattaché, s'appuyant sur les installations, les capacités administratives et le cadre réglementaire qu'elle met à sa disposition pour passer des contrats, recruter, ouvrir des crédits et fonctionner dans la pratique.

142. **La structure de gouvernance complexe est à l'image du rôle de prestataire de services axés sur les besoins de la clientèle.** Afin que son offre reste en phase avec les besoins des clients qu'il sert, le CIC établit son catalogue de services en collaboration étroite avec des représentants de ses organisations partenaires, dans le cadre de son comité de gestion. Cet organe de 41 membres ne représente pas la totalité de la clientèle du Centre, une distinction étant faite entre les organisations partenaires et les utilisateurs de ses services, qui ensemble constituent ses clients[50]. Seules les premières sont membres du comité de gestion, avec droit de vote, et ont leur mot à dire sur les lignes de services que le Centre est chargé de mettre au point, tandis que les clients qui n'ont pas la qualité d'organisation partenaire (les simples « utilisateurs ») ne peuvent s'abonner qu'aux services existants, qui ont déjà été mis au point. En outre, selon la formule du service optionnel, tous les membres du comité de gestion ne sont pas clients des services de cybersécurité et vice-versa (annexe VIII).

[50] Selon la modification apportée en 2003 au mémorandum d'accord portant création du Centre de calcul international, l'expression « organisations partenaires » s'entend de toute entité des Nations Unies qui utilise ses services et a été acceptée en qualité d'organisation partenaire par le comité de gestion, tandis que le terme « utilisateurs » désigne les gouvernements, les organisations intergouvernementales non partenaires, les ONG et les autres entités gouvernementales habilitées par le Directeur à utiliser les services du Centre.

Cette configuration présente par conséquent le risque d'entraver la mise au point ou l'amélioration des services dont une partie seulement des entités des Nations Unies ont un besoin concret. En ce qui concerne les services de cybersécurité en particulier, un groupe consultatif informel a été mis sur pied en 2020, constitué des trois entités qui contribuent le plus au financement des services de cybersécurité (actuellement le PNUD, le HCR et la FAO), avec pour objectif de suivre l'offre de services sur le plan de la qualité et de la pertinence, et de déceler de nouvelles possibilités de solutions partagées. Le groupe communique directement avec le responsable des services de cybersécurité du Centre, bien que le dernier mot en ce qui concerne la conception de nouveaux services reste du ressort du comité de gestion. Dans l'ensemble, l'architecture du Centre est apparue complexe, à l'image de la configuration en plusieurs couches de son modèle d'activité actuel. Il n'a pas été évident de répondre à la question de savoir si, dans sa forme actuelle, cette architecture était à même d'absorber et d'assumer correctement un rôle plus important, même mandaté, vis-à-vis du système. Certains des défis à relever à cet égard sont examinés plus en détail dans la section D du présent chapitre.

143. **Les avantages et les écueils du modèle d'activité du CIC.** Une fois qu'un service est prêt à être déployé, tous les clients qui s'y abonnent s'acquittent de droits d'utilisation, lesquels sont fixés et revus annuellement par le comité de gestion. La révision se fait habituellement à la baisse en fonction des économies d'échelle réalisées au fur et à mesure que de nouveaux clients s'abonnent au service en question, réduisant ainsi son coût pour chacun des abonnés. De ce point de vue, la stricte application du principe de récupération des coûts a l'avantage de garantir une tarification des services d'une grande transparente, d'imposer une coordination continue avec les clients et de contrôler l'étendue de l'offre de services dès lors qu'un alignement aussi précis que possible est nécessaire entre ce qui est réellement requis, d'une part, et ce qui est conçu et produit en conséquence, d'autre part. Un modèle commercial qui serait axé sur le profit est donc pour ainsi dire exclu, et c'est là un des aspects qui distingue le Centre des autres prestataires. Cela étant, aucun budget en tant que tel n'est prévu pour financer ses principales fonctions exécutives et administratives[51], de sorte que le financement de ces postes doit être inclus dans les droits d'utilisation des services proposés. Le modèle d'activité, qui combine les principes de récupération des coûts et de services partagés, s'est avéré à la fois favorable et contraire à la réalisation du projet du Centre de devenir une plaque tournante de la cybersécurité pour le système. Il a conduit à une situation dans laquelle l'offre de services du Centre dépend du financement d'amorçage que des clients peuvent consacrer à la conception d'un nouveau service répondant à la demande, alors que de nombreux clients ne pourront se permettre d'acquérir le service ainsi conçu que lorsqu'une masse critique de clients s'y seront abonnés. Cet état de choses a le potentiel de désavantager systématiquement les institutions financièrement moins puissantes, dont les besoins en cybersécurité peuvent différer de ceux de leurs pairs dont la souplesse budgétaire autorise le préfinancement de certains services.

Catalogue des services de cybersécurité

144. **Le CIC, acteur de premier plan du paysage de la cybersécurité des Nations Unies.** Ces dernières années, le Centre s'est affirmé en tant que partie prenante et ressource de premier plan de la cybersécurité pour les Nations Unies. Comme attesté par nombre de ses clients, le Centre a accumulé des connaissances spécialisées et des capacités considérables en matière de cybersécurité, et a graduellement étoffé son offre pour proposer 13 services spécialisés dans ce domaine, génériquement connus sous le nom de marque Common Secure (fig. IX et annexe VII). Les services, qui couvrent à la fois la gouvernance et les aspects opérationnels de la cybersécurité, sont proposés par le Centre en tant que fournisseur de services d'hébergement d'infrastructure assurant également la sécurité des données, systèmes et applications ainsi hébergés, que fournisseur de services de cybersécurité à part entière, que conseiller pour les questions de stratégie et de gestion, et qu'intervenant direct en cas d'incident, selon le type de service visé par l'abonnement. La versatilité de l'offre en matière de cybersécurité reflète le fait que la demande de ce type de services a sensiblement augmenté parmi les clients du Centre. Même si ces produits ne représentent qu'une fraction du

[51] Rapport et états financiers du Directeur du Centre international de calcul pour l'exercice biennal 2016-2017, publiés en avril 2018, p. 46 (en anglais).

catalogue de services du CIC, et à peine 6,1 % de son volume total de financement (selon les données de janvier 2021), les abonnés (actuels et anciens) à ces produits comptent 45 organisations, dont 21 sont des entités membres du CCS (qui en compte 31 en tout) et 20 sont des entités participantes du CCI (qui en compte 28 en tout). En dépit du fait qu'environ un tiers des entités de part et d'autre ne font pas partie des clients de ce type de services, à commencer par le Secrétariat de l'ONU, il est difficile de concevoir la cybersécurité dans le système des Nations Unies aujourd'hui sans prendre en compte le rôle et la contribution du Centre dans ce domaine.

Figure IX
Aperçu des services de cybersécurité du Centre international de calcul (2021)

Services	*Nombre d'entités participantes du Corps commun d'inspection (clients anciens et actuels)*
Service Common Secure de renseignements sur les menaces	17
Service commun de signature électronique	14
Intervention en cas d'incident	11
Services de gouvernance et d'appui aux responsables de la sécurité de l'information	11
Sensibilisation à la sécurité de l'information	10
Gestion des vulnérabilités	7
Tests d'intrusion	7
Services de simulation d'hameçonnage	6
Centre commun des opérations de sécurité	5
Évaluation de la sécurité de l'informatique en cloud (ou en nuage)	5
Infrastructure commune à clés publiques	3
Gestion des identités et des accès	3
Service Common Secure de gestion des informations et événements de sécurité	1

145. **Le service Common Secure de renseignements sur les menaces, produit phare du CIC.** Parmi les 13 services de cybersécurité proposés par le Centre, certains ont déjà attiré un nombre considérable de clients au sein du système des Nations Unies et au-delà, tandis que d'autres doivent encore se trouver une clientèle. Le service Common Secure de renseignements sur les menaces (*Common Secure Threat Intelligence*), service particulièrement populaire du Centre auquel sont abonnées 17 entités participantes, peut être considéré comme son produit phare dans le domaine de la cybersécurité, et une manifestation de son utilité. Il a recueilli des appréciations particulièrement positives de la part d'une bonne majorité des clients du Centre et répond à un besoin collectif de longue date et souvent reformulé au niveau du système. Il combine diverses sources internes et externes, notamment commerciales et gouvernementales, de renseignements sur les menaces. Les renseignements sont analysés et filtrés par le Centre pour produire des dossiers d'information digestibles, spécialement conçus pour l'environnement et le public des Nations Unies. À une session spéciale consacrée à la cybersécurité en octobre 2020, le comité de gestion du Centre a approuvé une résolution demandant à toutes les organisations partenaires et à tous les clients de communiquer à l'équipe Common Secure, de façon anonyme ou non, les renseignements sur les menaces et les informations sur les incidents de sécurité dont ils disposaient, de sorte que ces éléments puissent être analysés aux fins de leur diffusion au sein du système des Nations Unies. Les Inspecteurs saluent cette décision, mais constatent, sur la base des informations reçues, qu'elle doit encore être appliquée de façon généralisée. Pour la plupart des entités participantes sujettes de l'étude du CCI, c'est précisément un domaine qui se prêterait à une collaboration plus étroite à l'échelle du système, certaines faisant observer qu'outre la mise en commun de renseignements sur les menaces, parmi lesquels les indicateurs de compromission en particulier, il serait utile d'échanger des informations sur les mesures concrètes de riposte et de reprise qui étaient prises. Cet aspect des choses ne recueillait toutefois pas l'assentiment général des spécialistes interrogés par les Inspecteurs,

principalement pour des motifs de confidentialité. Il n'en reste pas moins que le service Common Secure de renseignements sur les menaces peut être considéré comme le service de cybersécurité le plus prometteur en ce qu'il a le potentiel d'être adopté de façon naturelle par tout le système et d'apporter à celui-ci de véritables gains de protection, au-delà même de ce qu'il réalise déjà aujourd'hui. Le même potentiel ne peut être reconnu aussi manifestement à toute la gamme des services de cybersécurité du Centre.

146. **L'évaluation des services de cybersécurité du CIC produit des résultats inégaux.** Malgré le contrôle rapproché que les clients exercent − pour des raisons structurelles − sur les services que leur propose le Centre, le retour d'information des entités participantes concernant leur degré de satisfaction vis-à-vis de ces services était plutôt inégal, allant de « très satisfait » à « très insatisfait ». Ce fait peut s'expliquer par plusieurs facteurs. D'une part, les appréciations données par les 20 entités participantes qui sont ou ont été abonnées à au moins un des services de cybersécurité du Centre ne portaient pas nécessairement sur les mêmes services ou le même nombre de services. Les différents degrés de maturité des cadres de cybersécurité de ces entités peuvent également avoir affecté la mesure dans laquelle chacune avait pu tirer parti de tous les aspects du service fourni. D'autre part, certains des services qui sont aujourd'hui proposés séparément étaient auparavant regroupés et disponibles sous forme de forfait, ce qui en soi avait suscité une certaine critique de la part des entités qui n'avaient eu d'autre choix que de s'abonner à des éléments dont elles n'avaient pas besoin pour obtenir ceux dont elles avaient besoin ou qu'elles souhaitaient. Le Centre aurait mis fin à cette pratique en 2019 et laisse aujourd'hui toute flexibilité à ses clients dans le choix du niveau et du type de service qui leur convient le mieux. En outre, une note d'appréciation de base peut être le reflet d'une impression plus générale de l'interaction avec le Centre, ou d'un autre aspect de l'expérience de l'entité, et risque dès lors d'être moins fiable et de ne pas être assez nuancée pour être concluante. Étant donné ces réserves et le fait que les Inspecteurs n'avaient pas pour but d'évaluer l'efficacité de chaque service du Centre ni de l'ensemble de son catalogue de services, il n'a pas été possible de dégager de correspondance entre le type, la taille et la maturité des entités et leur jugement plus ou moins critique du Centre. Globalement, il est permis de dire qu'un certain nombre d'entités, grandes et petites, ont apprécié le CIC au plus haut degré, et qu'un nombre égal ont adopté une position très critique à son égard. Cette position peut, dans certains cas, tenir à d'anciennes carences qui peuvent avoir été résolues par des évolutions subséquentes et qui ne devraient donc pas occulter le potentiel actuel et futur du Centre en tant prestataire de services de cybersécurité. Cela dit, les réserves exprimées peuvent très bien être d'actualité, d'une validité continue ou même récurrentes au fil du temps, et doivent par conséquent être prises très au sérieux. En tout état de cause, des évaluations régulières et précises de la satisfaction des clients peuvent donner des indications utiles sur les points à améliorer pour répondre aux préoccupations des clients et peuvent à terme lui amener de nouveaux clients. Qui plus est, une évaluation complète du Centre en tant que prestataire de services de cybersécurité peut s'avérer intéressante pour se faire une idée plus objective de la qualité et de l'adéquation de sa ligne de services dans ce domaine.

147. **Les avantages perçus d'un recours au CIC.** Les raisons qui plaidaient en faveur d'un recours aux services du Centre, telles que citées par ses clients, comprenaient la connaissance approfondie qu'il avait du système des Nations Unies et des besoins de ses entités, pour lesquelles il concevait depuis longtemps des services sur mesure, le fait qu'il était soumis aux mêmes règles et structures administratives, et sa participation à des plateformes interentités pertinentes. Le Centre a en outre relevé plusieurs avantages comparatifs qui le distinguaient des prestataires de services commerciaux, notamment la réduction du coût des services au fur et à mesure que croissait la clientèle, l'absence de but lucratif et, comme corollaire, la motivation de maintenir les prix à un niveau abordable, y compris pour les organisations moins nanties à la recherche de solutions à bas prix, l'objectif inhérent et partagé de rendre le système plus sûr pour tous, y compris pour lui-même en tant que membre, et la capacité d'observer ses clients, d'adapter ses produits en conséquence et de tirer de cette interaction des enseignements qui seront extrapolés pour le bien de la collectivité. La vue d'ensemble que le Centre a du système, en toutes ses composantes, le distingue également des fournisseurs commerciaux, qui souvent ne voient qu'une partie du tableau, et fait que la valeur ajoutée par ses services dépasse le cadre individuel de tel ou tel client. Les Inspecteurs ont également été frappés par le fait que, malgré

les mécanismes interentités en place et la couche supplémentaire de gouvernance représentative constituée par le comité de gestion du Centre, il ne s'était pas trouvé une seule entité intrinsèquement animée par la recherche de l'intérêt distinctement collectif du système plutôt que par les intérêts individuels, au mieux cumulés − et souvent inconciliables −, de ses membres. À cet égard, le Centre se voulait le courtier neutre, non politisé et − de par son modèle de récupération des coûts − désintéressé de solutions à l'échelle du système, guidé en cela par le bien commun plutôt que par certains des impératifs liés au manque cuisant de ressources qui pourraient orienter certains membres de son comité de gestion et les empêtrer dans un éventuel conflit d'intérêts.

148. **Les lacunes perçues du CIC en tant que fournisseur de cybersécurité.** À l'opposé, plusieurs entités ont porté un jugement moins favorable sur le Centre en tant que fournisseur de cybersécurité, critiquant en particulier le rapport coût-avantage de ses services par rapport à ceux que pourraient proposer des fournisseurs commerciaux, certaines ayant également l'impression que des services externes seraient en mesure de mobiliser des compétences techniques et des outils d'un niveau de perfectionnement que ne pourrait égaler le Centre ou une autre organisation, même moyennant d'importants investissements. D'autres voix au sein de la clientèle sont venues tempérer ces impressions, évoquant le bond en avant qu'ont connu, ces dernières années, les compétences techniques et la capacité de réaction du Centre dans le domaine de la cyberrésilience, comme l'attestent les importants investissements consacrés par sa direction aux mesures de conformité et de certification relatives aux normes ISO, au recrutement diversifié de spécialistes et à la mise sur pied d'un centre des opérations de sécurité partagé qui avait fonctionné sans arrêt, autant de mesures qui avaient contribué à développer les capacités de surveillance permanente du Centre et à étoffer son catalogue de services. Ces efforts ne sauraient toutefois escamoter la perception persistante qu'il reste en matière de compétences spécialisées et de rapport coût-avantage un fossé qui est − effectivement peut-être − difficile à combler pour le Centre. Il a également été relevé que des services similaires étaient disponibles à des prix plus concurrentiels auprès du secteur privé, et certains répondants estimaient que, en dépit des économies d'échelle découlant du modèle des services partagés, le Centre facturait certains de ses services à des prix trop élevés, et d'une façon peu transparente, ce qui les rendait inabordables ou trop opaques pour certaines entités, et pas assez amortis par des avantages dans certains domaines pour d'autres. En fait le Centre a reconnu qu'il n'avait pas les moyens, et que ce serait même contre-productif à certains égards, de concurrencer le secteur privé. Vu son modèle d'activité, le coût de ses services serait généralement réduit s'il y avait plus de clients, mais dans bien des cas, c'est aussi le coût qui fait obstacle à certaines entités qui souhaitent s'abonner aux services. Ce paradoxe pourrait être levé si, par exemple, des fonds moins strictement régis pouvaient être injectés aux bons endroits de sorte que le Centre puisse réduire certains de ses droits d'utilisation, éventuellement au-dessous de ceux que facturent les prestataires du secteur privé, sans avoir à les récupérer en totalité. Sachant qu'il ne sert à rien de vouloir concurrencer le secteur privé sur des terrains où celui-ci ajoute plus de valeur et est plus efficace, les chefs de secrétariat devraient se demander si le Centre pourrait servir d'interface entre les fournisseurs commerciaux et leurs clients du système des Nations Unies afin d'obtenir des prix plus intéressants, de réaliser des économies d'échelle et, en définitive, de gagner en pouvoir de négociation. De plus, et en conjonction avec l'évaluation indépendante de ses services de cybersécurité suggérée ci-dessus, le Centre souhaitera peut-être entreprendre une analyse critique de son catalogue de services de cybersécurité pour mettre en évidence les services qui lui confèrent un plus grand avantage relatif et leur consacrer plus d'efforts. En définitive, les Inspecteurs ont constaté que les critiques parfois dures dont le Centre faisait l'objet en tant que fournisseur de services de cybersécurité n'empêchaient pas le système des Nations Unies de tirer parti de son offre.

149. **Les possibilités d'amélioration du CIC dans le cadre de son mandat actuel.** Bien que certaines entités aient préconisé un renforcement formel du rôle du Centre en tant que prestataire de cybersécurité pour le système des Nations Unies, les Inspecteurs estiment que d'importants progrès peuvent d'ores et déjà être accomplis dans le cadre de son mandat actuel, tel qu'il a été révisé en 2003. En effet, celui-ci offre déjà une bonne base sur laquelle des solutions pourraient être mises en œuvre avec un peu plus de participation active de toutes les parties prenantes. Même si des raisons pertinentes rendaient nécessaires des modifications de son mandat, celles-ci seraient du ressort collectif des entités fondatrices et des entités qui

avaient adhéré à la modification de son acte constitutif en 2003, sans qu'il soit nécessaire de saisir l'Assemblée générale en attendant que soit réalisée, à la demande de celle-ci, une analyse plus exhaustive du Centre en tant qu'entité, de ses réalisations à ce jour et des raisons structurelles à l'origine de son potentiel non réalisé. De l'avis des Inspecteurs, il faudrait s'atteler sans attendre et sans condition préalable à la compréhension et à la résolution du décalage constaté entre les structures et mécanismes existants et certaines contraintes liées aux modalités de financement en vigueur, comme exposé ci-dessous.

D. Le renforcement des liens systémiques entre orientation stratégique et capacités opérationnelles

La résolution du décalage institutionnel entre le Groupe d'intérêt pour la sécurité informatique et le CIC

150. **La relation entre le Groupe d'intérêt pour la sécurité informatique et le CIC est limitée de façon formelle.** Compte tenu du chevauchement considérable entre les entités représentées dans les mécanismes de coordination interentités, d'une part, et le comité de gestion du CIC, d'autre part (annexe VIII), l'on serait fondé à présumer que le Groupe d'intérêt est l'organe qui fournit les orientations et les directives relatives aux solutions de cybersécurité partagées susceptibles de convenir aux entités des Nations Unies, tandis que le Centre fonctionne comme le bras opérationnel du système, chargé de la mise en application des orientations et directives. Les deux entités ne sont pourtant pas officiellement liées, pas plus qu'elles ne fonctionnent conjointement dans la pratique. Officiellement, le Groupe d'intérêt lui-même a pour seul rôle de partager l'information et de coordonner. Il n'est en aucune façon mandaté pour donner des instructions au CIC ; celui-ci exécute les décisions de son propre comité de gestion s'agissant de concevoir des services pour ses clients, lesquels ne comprennent pas toutes les entités des Nations Unies. Dans la pratique, le décalage institutionnel entre les deux organes n'est peut-être pas le facteur décisif, mais il a probablement contribué à une dynamique qui peut coûter cher au système en gains d'efficience non réalisés, à cause des occasions manquées de collaboration plus directe.

151. **Les interactions sont tendues dans la pratique, pour une série de raisons.** En réalité, le CIC s'est vu octroyer la qualité d'observateur au sein du Groupe d'intérêt pour la sécurité informatique et il participe aux discussions qui s'y tiennent, sans avoir le droit de voter ni de soumettre des sujets à discussion. Le Centre a toutefois déclaré qu'il avait effectivement été privé de la possibilité de promouvoir son catalogue de services dans le cadre du Groupe d'intérêt ou d'y recueillir directement des avis sur ses solutions. Cette situation peut s'expliquer en partie par la nature du Centre en tant que dispositif interentités et non en tant qu'entité ayant qualité pour devenir membre du CCS et jouir de pleins droits de participation. Il a également été question de la perception sous-jacente selon laquelle le Centre tenait plus d'un fournisseur que d'un partenaire pour les entités du système, ce qui rendait encore plus improbable l'idée d'une pleine intégration dans les mécanismes interentités existants. Compte tenu du modèle d'activité du CIC, axé sur le client, et de son rôle de fournisseur de services sur mesure à ses organisations partenaires, il serait difficile de ne pas reconnaître quelque fondement à son image de fournisseur. Cela étant, il se présente ouvertement comme une entité des Nations Unies et un membre à part entière de son système. En fait, la direction du Centre a clamé haut et fort sa volonté d'en faire la plaque tournante du système en matière de cybersécurité si la possibilité lui en était donnée, certaines entités allant même, pour leur part, jusqu'à penser qu'il devrait faire de la cybersécurité son métier principal. Ce scénario risque toutefois de rester illusoire tant que n'auront pas été abordés et résolus les obstacles tenant à la dynamique entre les mécanismes interentités établis au sein du système et Centre en tant que prestataire privilégié de services de cybersécurité ayant le potentiel d'assumer le rôle de composante opérationnelle du système dans ce domaine.

152. **Les structures sont de facto parallèles.** L'exemple de la conférence Common Secure, organisée par le CIC, montre comment la dynamique entre le dispositif interentités et le CIC peut tout à la fois produire des solutions spontanées à des besoins avérés et créer des situations de double emploi dans le domaine de la cybersécurité. Depuis 2019, la conférence permet aux clients des services de cybersécurité du Centre d'échanger des informations sur des questions d'intérêt commun au niveau opérationnel ainsi que de faire

part de leurs observations sur les services fournis. Devenue une manifestation récurrente et bien considérée du calendrier de la cybersécurité, elle est très appréciée de ses participants parmi lesquels figurent de nombreuses entités des Nations Unies qui sont aussi représentées au sein du Groupe d'intérêt pour la cybersécurité. D'une certaine façon, on peut dire que la conférence Common Secure comble une lacune pour le Centre, qui avait cherché à se concerter avec les organisations dans le cadre du Groupe d'intérêt, sans pour autant arriver à le faire d'une façon aussi productive et concrète qu'il l'aurait souhaité s'agissant de son objectif d'améliorer le partenariat avec le système et les aspects opérationnels de son offre de services. D'aucuns pourraient même dire que la conférence est devenue la principale plateforme à cet égard pour une grande partie du système, en conséquence directe de l'incapacité du Groupe d'intérêt en tant que mécanisme de coordination actuel de donner corps à un débat plus orienté vers les solutions. Il est vrai que cette évolution dynamique et innovante a peut-être aussi eu l'inconvénient de détourner certaines discussions qui auraient très bien pu avoir eu lieu au sein du Groupe d'intérêt vers une autre plateforme qui, en théorie, s'adresse plus aux clients du Centre qu'au système dans son ensemble. La coexistence de ces deux structures − plus parallèles que complémentaires, à vrai dire − aux objectifs largement similaires, l'une sous les auspices du CCS et l'autre sous ceux du Centre, risque de créer un décalage et une concurrence supplémentaires, sources d'inefficacités, de doubles emplois et de chevauchements. C'est là un des effets secondaires dommageables de la dynamique entre les deux parties et de sa gestion qui laisse à désirer.

153. **Les synergies devraient être développées.** Ces observations devraient éclairer les actions de deux entités en vue d'améliorer la façon dont elles interagissent. D'une part, le Groupe d'intérêt pour la sécurité informatique doit redoubler d'efforts, en tant que structure collégiale, pour exécuter son mandat dans un sens plus stratégique, relevant les domaines propices aux solutions partagées, si ce n'est pour le système dans son ensemble, du moins pour des groupements d'entités dont les dispositifs de cybersécurité améliorés élèveraient celui du système. S'il s'abstient de suivre de cette voie et d'user ce faisant de la voix autorisée qui est la sienne au nom du système, il y a de grandes chances pour que le Centre soit forcé de monter en piste et d'occuper cet espace tout en restant limité au cercle des clients qu'il sert. En revanche, le fait pour le Centre de tirer parti de ce vide créé par inadvertance par le Groupe serait, en principe, une bonne chose pour le système, car il serait porteur d'innovation. Mais cela ne devrait pas se faire à l'écart de l'organe officiel chargé de la coordination et de la coopération en matière de cybersécurité à l'échelle du système. Il est de la responsabilité des deux parties de s'employer à rechercher des moyens formels ou informels par lesquels améliorer la dynamique qui existe entre elles. Un certain nombre de services de cybersécurité largement utilisés dans le catalogue du Centre sont considérés comme ayant été inspirés ou directement produits par des échanges qui avaient eu lieu dans le cadre du Groupe d'intérêt, même sans avoir été formellement commandés par celui-ci. Si le Centre reste résolu à poursuivre son chemin vers le rôle de plateforme de la cybersécurité pour l'ensemble du système plutôt que pour ses propres clients seulement, il ne peut se permettre de rester détaché de la communauté de spécialistes qui représente les besoins collectifs des entités qu'une telle plateforme serait amenée à servir. Qui plus est, en tant que structure collégiale, le Groupe d'intérêt détient une partie de la clé s'agissant de faciliter une collaboration plus constructive dans ce domaine. Le potentiel existe pour de plus amples synergies et une plus grande complémentarité, mais il n'a pas encore été pleinement réalisé à ce jour.

154. **Les organisations participantes devraient se reposer la question de l'utilisation des services de cybersécurité du CIC.** Une solution suggérée par certains pour résoudre le décalage entre les deux entités serait de rendre les services de cybersécurité du Centre obligatoires pour toutes les entités des Nations Unies. Il a été fait valoir que cette solution accélérerait aussi les gains d'efficience et les réductions de prix en renforçant la portée et la profondeur du travail du Centre en tant fournisseur de services partagés. Cette façon de voir les choses ne faisait pas l'unanimité et pourrait bien s'avérer contre-productive dans la pratique. D'une part, elle réduirait l'autonomie dont les entités des Nations Unies jouissent pour évaluer et choisir les offres de services qui répondent le mieux à leurs besoins, et elle conduirait à une monopolisation du fournisseur et de l'offre de services vers l'extérieur. D'autre part, le Centre dispose de mécanismes de gouvernance qui permettent déjà de sains échanges entre sa direction exécutive et ses clients concernant la forme à donner aux services

de cybersécurité. Les Inspecteurs estiment qu'il n'est ni prudent ni nécessaire d'intervenir dans ces mécanismes. **Dès 2019 cependant, les Inspecteurs ont encouragé les entités des Nations Unies et le CIC à élargir leurs domaines de coopération pour que les premières puissent compléter leurs capacités internes au moyen de services partagés supplémentaires**[52]**.** Les Inspecteurs estiment en particulier que certaines des raisons qui, par le passé, peuvent avoir amené des entités à se désabonner des services du Centre ou à ne pas s'y abonner du tout, mériteraient d'être réexaminées. La décision de procéder à tel réexamen devra être nuancée, chaque service de cybersécurité proposé devant idéalement être (ré)évalué séparément. De fait, certains services n'ont peut-être pas encore acquis la maturité ou la réactivité nécessaires pour répondre aux besoins des organisations et justifier que toutes s'y abonnent. Il appartient au Centre de poursuivre ses efforts pour combler toute lacune de cet ordre. Les Inspecteurs reconnaissent également l'individualité de chaque organisation. En définitive, c'est aux organisations elles-mêmes qu'il appartient de prendre les décisions voulues en fonction de leurs besoins propres, compte tenu notamment de la grande diversité des systèmes informatiques, des applications et d'autres dispositions techniques à caractère interne ou prises sous contrat avec des fournisseurs externes.

La solution des contributions volontaires de donateurs pour compléter le financement des solutions partagées destinées au système

155. **Les contributions volontaires en appui direct.** De l'avis des Inspecteurs, le moment est opportun pour envisager le recours aux contributions volontaires en tant que mécanisme de financement complémentaire, afin de disposer de ressources qui puissent être affectées plus directement à la préservation du dispositif global de cybersécurité du système. La disponibilité de contributions volontaires spécifiquement destinées au financement de mesures à l'échelle du système pourrait lever certains des obstacles à la mise en œuvre de solutions de cybersécurité partagées, étant probable que le manque de ressources au sein des organisations participantes a affecté leur disposition à contribuer à un fonds commun. La possibilité pour le système de puiser à une source de contributions de donateurs qui soit indépendante des budgets respectifs de ses membres pourrait soulager les pressions résultant, d'une part, de la très faible marge de manœuvre prévue dans lesdits budgets, appelés à satisfaire une telle quantité de priorités institutionnelles en concurrence pour des fonds toujours plus limités et, d'autre part, du modèle de récupération des coûts pratiqué par le CIC. Dans ce dernier cas, les contributions volontaires pourraient ouvrir la voie à la mise au point de lignes de services innovantes à l'intention des organisations partenaires, surtout celles dont les capacités internes sont moins développées ou qui disposent de ressources moindres pour s'occuper de leur cybersécurité en général. Combinée avec le modèle des services partagés, cette démarche contribuerait à la maîtrise des coûts en maintenant les droits d'utilisation à un niveau peu élevé, et attirerait probablement de nouveaux clients, ce qui multiplierait les effets positifs. En consultation avec les interlocuteurs concernés, les Inspecteurs se sont intéressés à la question de savoir si le mécanisme de collecte et de débours des contributions volontaires envisagées serait plus avantageusement placé sous l'autorité du système lui-même, à titre collectif, sous la forme d'un fonds d'affectation spéciale administré par le CCS avec le bénéfice de la contribution technique du Groupe d'intérêt pour la sécurité informatique, ou par le CIC en tant que fournisseur de facto et bien établi de nombreuses solutions partagées pour le système. S'étant penchés sur diverses possibilités, les Inspecteurs ont conclu que ce fond serait le plus avantageusement rattaché à l'entité qui devrait pouvoir assurer un suivi opérationnel, au jour le jour, des dépenses engagées dans la mise au point des services souhaités, à savoir le CIC.

156. **Un fond d'affectation spéciale pour la cybersécurité.** En principe, depuis sa modification en 2003, le mandat du CIC contient des dispositions qui lui permettent de recueillir des contributions volontaires. Il y a également, eu ces dernières années, un précédent de projet particulier financé par cette voie. C'est un mécanisme qui a été sous-utilisé à ce jour, et son déploiement stratégique pour la conception anticipée de services destinés à être partagés par toutes les entités des Nations Unies ou plusieurs d'entre elles a la capacité de changer la donne. Moyennant une certaine publicité et l'affinement des conditions qui en régissent l'utilisation, cette formule pourrait donner l'occasion aux États

[52] JIU/REP/2019/5.

Membres qui souhaitent contribuer directement au renforcement de la cybersécurité dans l'ensemble du système de soutenir des solutions partagées à cette fin, conformément aux termes régissant l'affectation particulière de leur contribution. Elle faciliterait également l'application de la recommandation formulée par le CCI en 2019 tendant à ce que soit instauré un mécanisme de financement qui permette au CIC de mener des activités de recherche-développement en dehors des contraintes de son modèle de récupération des coûts, avec les avantages supplémentaires que cela pourrait comporter pour sa clientèle parmi les entités des Nations Unies. Les Inspecteurs recommandent par conséquent qu'à l'issue des consultations nécessaires, le Directeur du CIC créée un fonds d'affectation spéciale pour la cybersécurité dans le but précis de financer la conception et la mise au point des services de cybersécurité partagés dont le système a le plus besoin. Pour distinguer encore ce mécanisme d'autres sources de financement mises à la disposition du CIC par ses organisations partenaires et ses clients, la création d'un fonds d'affectation spéciale serait en effet la solution prudente en l'occurrence, assortie de conditions spéciales pour veiller à ce que sa gouvernance ne reproduise pas les déséquilibres structurels existants, d'éventuels conflits d'intérêts ou des dynamiques malvenues résultant du chevauchement de la composition de son comité de gestion et de celle des organes interentités correspondants à l'échelle du système.

157. **La mise en œuvre du fonds d'affectation spéciale.** Il suit de ce qui précède que le mandat d'un tel mécanisme de financement est déterminant pour les résultats qu'il va donner. Le mandat doit préciser les rôles et les responsabilités des différentes parties prenantes, les types de services que le fonds doit financer et les procédures à suivre pour allouer les fonds de façon transparente, y compris les obligations de communication associées. Il est particulièrement important que le fonds soit mis en place de telle sorte qu'il serve essentiellement à des fins qui soient tangibles pour les entités du système. Son objectif principal pourrait être de financer des activités de recherche-développement qui visent le lancement de services de cybersécurité pour lesquels il y a un intérêt certain parmi les entités, mais qu'il faille compter sur une masse critique de clients prêts à se répartir le financement de départ requis. De même, le fonds pourrait être utilisé pour étendre la portée ou la profondeur des services existants pour lesquels il y a une demande manifeste et qui nécessitent un financement de départ, ou dont le prix devrait être revu à la baisse pour permettre à un plus grand nombre d'entités de s'y abonner plus tôt. Bien qu'en général, les règles de financement de l'OMS, organisation hôte du CIC, devraient d'appliquer, il serait également possible d'inclure dans la gouvernance du fonds un élément de consultation avec les organes interentités compétents. Ceci contribuerait à la conception de solutions partagées qui seraient mises au point pour le système dans son ensemble plutôt que pour les seuls clients du CIC, et améliorerait encore l'exploitation des ressources disponibles. Étant donné qu'elle a jeté les bases de la création du CIC, l'Assemblée générale est invitée à prendre acte de la recommandation visant l'instauration d'un fonds d'affectation spéciale et à engager les États Membres à y contribuer.

158. L'application des recommandations suivantes devrait renforcer la coordination et la coopération parmi les entités des Nations Unies.

Recommandation 3

Le Directeur du Centre international de calcul des Nations Unies devrait s'employer à établir, d'ici à la fin de 2022, un fonds d'affectation spéciale destiné à recevoir les contributions des donateurs souhaitant renforcer les capacités du Centre en matière de conception, de mise au point et de prestation de services et de solutions partagés visant à développer le dispositif de cybersécurité des entités des Nations Unies.

Recommandation 4

L'Assemblée générale des Nations Unies devrait, au plus tard à sa soixante-dix-septième session, prendre acte de la recommandation adressée au Directeur du Centre international de calcul des Nations Unies d'établir un fonds d'affectation spéciale pour les solutions de cybersécurité partagées, et inviter les États Membres qui souhaitent renforcer le dispositif de cybersécurité des entités des Nations Unies à contribuer au fonds.

E. Les possibilités d'harmoniser davantage sécurité physique et cybersécurité

159. **La cybersécurité n'est pas incluse dans le système de gestion de la sécurité des Nations Unies.** L'Assemblée générale a créé le Département de la sûreté et de la sécurité dans sa résolution 59/276 et l'a chargé de définir, à l'échelle du système, le cadre directeur, le cadre des responsabilités, les normes opérationnelles et les procédures opérationnelles régissant la sûreté et la sécurité du personnel et des actifs des Nations Unies. Il n'est sans doute pas surprenant que le mandat confié au Département de la sûreté et de la sécurité en 2004, avant que la cybersécurité n'ait franchi les étapes marquantes de 2013 et de 2014 à l'échelle du système, ne fasse pas référence à la protection des données et des actifs numériques ou, d'un point de vue plus large, au cyberenvironnement[53]. Bien que le Département ait confirmé que les consignes relatives à la sécurité de l'information étaient d'application dans tout le système des Nations Unies, le système de gestion de la sécurité des Nations Unies et les documents directifs qui y étaient associés devaient encore énoncer les points de convergence entre la sécurité physique et la cybersécurité, de sorte à déterminer les responsabilités des diverses parties prenantes à cet égard. Les Inspecteurs saluent l'inclusion d'un espace réservé à la sécurité de l'information, et plus précisément à la classification et au maniement des informations sensibles ou confidentielles, dans le Manuel des politiques de sécurité du système de gestion de la sécurité des Nations Unies. Ils y voient une certaine reconnaissance du fait que les considérations de cybersécurité sont pertinentes pour la fonction de sûreté et de sécurité physiques. Il reste que le chapitre en question doit encore être élaboré et que le Département de la sûreté et de la sécurité a exprimé des réserves quant à la nécessité, à ce stade, d'un chapitre distinct consacré à la question. En attendant, comme confirmé par le Bureau des affaires juridiques, et contrairement à l'interprétation établie selon laquelle les références à la protection des biens et des avoirs dans les conventions et dans les accords avec les pays hôtes s'entendent juridiquement des actifs et des communications numériques, ni le mandat ni le cadre directeur régissant la fonction de sûreté et de sécurité dans le système des Nations Unies ne peuvent être considérés comme incluant actuellement la cybersécurité.

160. **Le Réseau interorganisations pour la gestion des mesures de sécurité et le Groupe d'intérêt pour la sécurité informatique.** Il n'y a pas non plus de mention spécifique de la cybersécurité dans le mandat du Réseau interorganisations pour la gestion des mesures de sécurité qui épaule le Comité de haut niveau sur la gestion dans son examen complet des politiques et des questions de ressources relatives au système de gestion de la sécurité des Nations Unies et surveille la mise en œuvre des politiques, pratiques et procédures de gestion de la sécurité par tous les acteurs du système des Nations Unies. Les recherches effectuées par le CCI confirment que le Réseau n'a abordé le sujet qu'à de rares occasions et principalement du point de vue de l'utilisation des TIC pour renforcer les processus généraux de sécurité physique, comme la gestion des identités et des accès (et l'étude de l'utilisation des cartes biométriques pour contrôler l'accès aux espaces physiques et numériques) ou les procédures de certification assistée par les TIC en matière d'habilitation de sécurité pour les déplacements du personnel. Plus récemment, en 2019, une recommandation du Groupe d'intérêt pour la sécurité informatique relative à la mise en place

[53] Le Département de la sûreté et de la sécurité a précisé que son mandat ainsi que le système de gestion de la sécurité des Nations Unies portaient sur les troubles civils, les conflits armés, le terrorisme, les infractions et les risques et dangers (non délibérés).

de dispositions de coordination entre le Groupe d'intérêt et le Réseau interorganisations sur des questions d'intérêt commun a été adoptée par le Réseau Technologie et numérique[54]. Les Inspecteurs n'ont toutefois pas trouvé d'éléments tendant à établir qu'il avait été donné suite à cette déclaration d'intention en dehors de certains projets bien précis. Les mécanismes interentités compétents sont invités à explorer plus avant les modalités pratiques de la mise en place d'une voie de communication plus régulière qui permettrait une meilleure coopération. À cet égard, il a été suggéré aux Inspecteurs que la participation mutuelle des présidents du Réseau interorganisations et du Groupe d'intérêt aux réunions des deux entités pourrait faciliter l'échange des enseignements tirés de leurs expériences respectives.

161. **Un plan de coopération avec les autorités nationales en matière d'atteintes à la cybersécurité.** La coopération avec les autorités nationales en cas de cyberattaques est un des domaines où les procédures en vigueur en matière de sûreté et de sécurité physiques peuvent constituer des sources d'inspiration pour la sphère numérique. Dans le chapitre II (par. 35 à 37) du présent rapport, les Inspecteurs ont examiné de façon relativement approfondie les processus internes complexes qui conduisent à la décision de prendre contact avec les autorités nationales, sans parler de ce qui se produirait une fois qu'une telle décision aurait été prise ni de comment se déroulerait la communication avec les homologues gouvernementaux concernés. La question est loin d'être simple, car l'homologue le plus approprié au niveau national peut varier entre le ministère responsable des équipes d'intervention en cas d'atteinte à la sécurité de l'information (ministères de l'intérieur, de la défense, des communications ou de la technologie, selon les compétences) et les capacités parallèles qui peuvent exister dans le même État sous le ressort de l'agence nationale de renseignements lorsqu'elle est chargée de se saisir des cyberattaques dans un contexte qui peut être politique. C'est pourquoi il peut ne pas y avoir de point de contact central désigné au niveau national pour recevoir les rapports des entités des Nations Unies en la matière, ce qui peut compliquer le bon acheminement de l'information. À titre de consigne pour la gestion des crises touchant à la sécurité physique, le Manuel des politiques de sécurité du système de gestion de la sécurité des Nations Unies charge les responsables désignés de demander au gouvernement hôte de désigner des points de contact ayant autorité pour mobiliser et coordonner des mesures d'appui aux Nations Unies lorsqu'elles sont affectées par une crise dans le pays[55]. Une démarche analogue pourrait être envisagée dans le cadre du plan de collaboration en cas d'atteintes à la cybersécurité, sachant que les responsables désignés profiteraient dans ces cas des conseils spécialisés de la fonction de cybersécurité de leur entité.

162. **L'absence de mécanisme de transmission, de réception et d'acheminement de l'information relative au cyberespace au sein du système.** De même, il faudrait que des dispositions internes soient en place pour recevoir l'information relative au cyberespace provenant des gouvernements. La présence de telles dispositions n'est cependant pas apparue aux Inspecteurs dans le cadre de leur examen. Certains interlocuteurs ont laissé entendre qu'il y avait une certaine confusion parmi les homologues gouvernementaux quant à l'organisation avec laquelle ils devaient pendre contact lorsqu'il s'avérait qu'une cyberattaque détectée sur le plan national concernait aussi une ou plusieurs entités des Nations Unies, et quant à la voie de communication à utiliser dans ce cas. Il a été avancé que les renseignements de ce type étaient souvent disponibles et prêts à être partagés, mais qu'il n'existait aucun mécanisme pour les transmettre et les acheminer de façon fiable à qui de droit au sein du système, en particulier parce qu'il n'était pas évident pour des entités externes de savoir à quel membre du système se rapportaient les renseignements en question. Apparemment, cet état de choses s'était soldé par des occasions manquées de protéger et de défendre les actifs institutionnels contre des intrusions, faute de pouvoir faire en sorte que les renseignements relatifs au cyberespace atteignent un destinataire doté des compétences techniques nécessaires pour y donner suite. Les voies de communication diplomatiques établies ont par conséquent été jugées insuffisamment efficaces en ce qu'elles privaient les entités concernées et le système en entier d'avantages en matière de cybersécurité.

[54] CEB/2019/HLCM/DTN/02 et CEB/2019/HLCM/DTN/07, p. 4 et 5 (en anglais).

[55] Manuel des politiques de sécurité du système de gestion de la sécurité des Nations Unies, sect. D − Relations avec les pays hôtes concernant les questions de sécurité, par. 14 d), « Gestion des crises ».

163. **L'opportunité et l'adéquation d'une approche harmonisée.** Certains des facteurs conduisant au caractère inégal de la pratique actuelle des entités des Nations Unies en matière de coopération avec les autorités nationales sont expliqués aux paragraphes 35 à 37 ci-dessus. Se pose alors la question de savoir si les incohérences découlant de cet état de fait sont susceptibles de créer des difficultés supplémentaires, notamment des difficultés liées à la réputation dans la gestion des relations avec le pays hôte, à plus forte raison dans des situations où plusieurs entités des Nations Unies avec des démarches différentes ont un siège ou une présence dans le même pays et traitent − ou non − les questions de cybersécurité avec les mêmes autorités. **Les Inspecteurs demandent au Comité de haut niveau sur la gestion d'entreprendre une réflexion collective sur l'opportunité et l'adéquation d'une approche harmonisée de la coopération et des consignes y afférentes dans ce domaine.** Le Groupe d'intérêt pour la sécurité informatique, le Réseau interorganisations pour la gestion des mesures de sécurité et le Réseau des conseillères et conseillers juridiques sont bien placés pour apporter leurs compétences techniques à un examen conjoint de la question et se pencher sur les avantages possibles en matière de sécurité, les difficultés associées et, en particulier, la faisabilité de la désignation de points de contact institutionnels, y compris au niveau du système, avec pour tâches de transmettre, recevoir et acheminer les informations relatives aux menaces et aux risques touchant à la cybersécurité. Conscients de la participation du CIC au Réseau interorganisations pour la gestion des mesures de sécurité, les Inspecteurs ont noté que le Centre s'était dit prêt, si cette responsabilité lui était officiellement confiée, à jouer un rôle dans le regroupement et la communication des informations sur les atteintes à cybersécurité que les entités des Nations Unies destinaient aux autorités nationales. S'il est vrai que la communication d'informations aux autorités nationales et la coopération avec celles-ci sont des tâches du ressort de chaque entité, le fait que le CIC ait accès à des informations qui lui permettent de discerner l'existence éventuelle, entre différentes attaques dirigées contre différentes entités, de liens et d'interdépendances qu'aucune des entités concernées ne saurait sans doute établir seule, constitue certes un argument en faveur d'un rôle accru du Centre dans ce domaine et mérite plus ample examen. Lorsqu'ils s'intéressent à la possibilité d'une approche harmonisée à cet égard, les mécanismes interentités compétents devraient par conséquent inviter et étudier les contributions éventuelles des parties prenantes concernées, y compris le CIC, en particulier pour ce qui concerne la capacité de ce dernier de collecter, de mettre en corrélation et d'analyser, au nom du système, les éléments de preuve relatifs à une intrusion.

164. **Vers une meilleure harmonisation de la sécurité physique et de la cybersécurité.** De façon plus générale, vu que les directives de 1992 relatives à la sécurité de l'information formulées par le prédécesseur du Réseau Technologie et numérique évoquaient déjà les liens qui existaient entre la sécurité des systèmes informatiques et la sécurité physique[56], et que la question était revenue à l'ordre du jour dans les discussions des organes compétents en 2013 et 2014[57], les Inspecteurs estiment que le moment est venu de relancer les efforts tendant à mieux harmoniser les fonctions de sécurité physique et de cybersécurité afin d'assurer le plus haut degré de protection contre les menaces complexes. Le Département de la sûreté et de la sécurité, en tant qu'autorité centrale et normative pour tout le système, a un rôle crucial à jouer pour ce qui est de reconnaître les points de convergence existants et peut devenir un acteur de premier plan dans une évolution majeure de la culture institutionnelle. Dans le système des Nations Unies, les menaces à la sécurité physique sont déjà des préoccupations de la plus haute importance, et la nécessité de les contrer immédiatement et efficacement ne fait aucun doute. Bien que les Inspecteurs aient détecté une évolution prudente de la pensée institutionnelle en faveur d'une riposte revêtant le même degré d'urgence face aux menaces à la cybersécurité, il reste beaucoup à faire pour étendre de la sphère purement physique à celle du cyberespace l'approche axée sur la gestion des risques et la riposte structurée autour des responsabilités qui sont déjà propres au Département de la sûreté et de la sécurité. Cela ne veut pas dire qu'il faille revoir le mandat systémique dont est déjà investi le Département pour accommoder la cybersécurité. Les Inspecteurs reconnaissent que le défi moderne de contrecarrer les acteurs qui menacent la cybersécurité nécessite des ressources et des

[56] *Information System Security Guidelines for the United Nations Organizations*.

[57] CEB/2013/5, par. 40 ; dix-neuvième session du Réseau interorganisations pour la gestion des mesures de sécurité (2013, document sans cote) et vingtième session du Réseau interorganisations pour la gestion des mesures de sécurité (2014, document sans cote).

compétences techniques particulières dont ne dispose pas actuellement le Département de la sûreté et de la sécurité, et que le transfert d'une partie, quelle qu'elle soit, de cette responsabilité, ne saurait se concevoir sans d'importants ajustements. Toute évolution dans ce sens nécessiterait des modifications structurelles, y compris l'intervention de l'Assemblée générale, et d'importants exercices de consultation et de coordination avec les diverses parties prenantes du système de gestion de la sécurité des Nations Unies, notamment sur des questions de ressources administratives et financières et de relèvement des compétences du personnel de sécurité, comme il est fait valoir ailleurs dans le présent rapport (par. 68). Il ressort de l'examen qu'à l'heure actuelle, le débat sur cette question à l'échelle du système n'a pas atteint la maturité nécessaire. Il faudrait relancer les efforts dans ce sens et entreprendre un examen plus approfondi, en tirant parti des compétences techniques disponibles dans le système et notamment au niveau du Réseau interorganisations pour la gestion des mesures de sécurité et du Groupe d'intérêt pour la sécurité informatique. Les Inspecteurs recommandent par conséquent que le Secrétaire général étudie les possibilités d'exploiter davantage la convergence entre la sécurité physique et la cybersécurité au sein du système des Nations Unies, et qu'il recherche les avantages et les inconvénients des différentes façons d'arriver à cette fin. Le rapport adressé à l'Assemblée générale en la matière devrait, dans la mesure du possible, être éclairé par les résultats de consultations à mener entre les mécanismes interentités de coordination compétents saisis de la cybersécurité et le Réseau interorganisations de gestion des mesures de sécurité, moyennant la contribution du CIC, selon que de besoin.

165. L'application de la recommandation suivante devrait renforcer l'efficacité de la riposte du système des Nations Unies aux menaces à la cybersécurité.

Recommandation 5

Le Secrétaire général devrait présenter à l'Assemblée générale des Nations Unies, au plus tard à sa soixante-dix-huitième session, un rapport ayant pour objet d'étudier de nouvelles possibilités de mettre à profit la convergence entre la sécurité physique et la cybersécurité pour assurer une protection plus globale et intégrée du personnel et des actifs des Nations Unies, et d'indiquer, en conséquence, les mesures qui seraient nécessaires pour renforcer les structures existantes, en accordant une attention particulière au rôle que pourrait jouer le Département de la sûreté et de la sécurité à cet égard.

Annexe I

Les axes de travail intergouvernementaux relatifs à la cybersécurité et à la cybercriminalité

Introduction et termes utilisés

La communauté internationale a débattu de questions relatives à la cybersécurité dans plusieurs cadres intergouvernementaux.

D'une part, le sujet a été examiné par différentes commissions de l'Assemblée générale et par différents organismes rattachés ou associés à celle-ci. Un axe de travail portait sur la cybercriminalité (appelée criminalité informatique au début des années 1990) et l'autre sur l'information et les télécommunications dans le contexte de la sécurité internationale (ce qui comprenait la sécurité informatique et les sujets connexes).

D'autre part, les mandats de plusieurs entités participantes visent des aspects de la cybersécurité qui relèvent des processus intergouvernementaux soutenus par ces entités. Tel est le cas de l'UIT, du Bureau des affaires de désarmement de l'ONU, de l'ONUDC, de l'OMPI, du PNUD, de la CNUCED et de l'AIEA.

Les termes « cybercriminalité » et « cybersécurité » ne sont pas interchangeables, bien qu'ils abordent la même question sous des angles différents. L'on pourrait dire que la cybercriminalité met l'accent sur la perpétration de cyberattaques et sur la responsabilité pénale encourue par les attaquants du fait de leur participation à des activités illicites (faisant appel à l'informatique ou dépendantes de celle-ci). La cybersécurité se rapporte quant à elle au fait de se défendre contre de telles attaques, mettant ainsi la cible et ses défenses, plutôt que l'auteur, au centre des préoccupations.

La présente annexe donne un aperçu des axes de travail intergouvernementaux qui ont été poursuivis en la matière au niveau des entités des Nations Unies. Il est question de leurs origines, de leurs activités actuelles, ainsi que des relations qui existent entre eux, le cas échéant.

Axe de travail I : cybercriminalité

La cybercriminalité à l'ordre du jour mondial depuis les années 1990. Les premières traces documentaires d'une prise de conscience, au sein de la communauté internationale, de la nécessité d'accorder une attention particulière au cyberespace dans les activités relatives aux programmes, et d'investir dans la capacité des États de repousser les cyberattaques (avec l'appui technique des entités des Nations Unies concernées), remonte à 1990, dans le contexte de la lutte contre la criminalité transfrontalière. Dans sa résolution 45/121, l'Assemblée générale a accueilli avec satisfaction les recommandations du huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, et en particulier la résolution relative à la criminalité informatique invitant les États à intensifier leurs efforts pour lutter de façon plus efficace contre les utilisations abusives de l'informatique. Les travaux en la matière se sont poursuivis sous le titre « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles »[1] au sein de la Troisième Commission de l'Assemblée générale (Commission des questions sociales, humanitaires et culturelles) et sous le titre « Cybercriminalité » dans le contexte de la Commission pour la prévention du crime et la justice pénale (commission technique du Conseil économique et social). Ces travaux s'effectuent avec l'appui organique et administratif de l'ONUDC.

[1] Résolutions 73/187, 74/247 et 75/539 de l'Assemblée générale et, antérieurement, résolutions 55/63 et 56/121 de l'Assemblée générale.

Les travaux en cours vers une convention internationale relative à la cybercriminalité. Des efforts sont déployés depuis 2010 pour réaliser une « étude approfondie du phénomène de la cybercriminalité » dans le cadre du groupe intergouvernemental d'experts à composition non limitée convoqué à cette fin par la Commission pour la prévention du crime et la justice[2]. Le corpus de travaux qui en est résulté a gagné en ampleur et en maturité pour déboucher sur une entreprise à part entière tendant à l'établissement d'un instrument légalement contraignant relatif à la cybercriminalité. Le processus de rédaction et de négociation de l'instrument est supervisé par un comité spécial, créé par l'Assemblée générale en 2019, qui a entamé en 2020 sa mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles[3]. Le résultat de ce processus sera principalement considéré par les États en tant que parties à la convention qui en résultera. Le cadre juridique qu'il pose est surtout destiné à régir le traitement des auteurs individuels (les cybercriminels) au niveau national, et n'a donc guère d'incidence sur la démarche des entités des Nations Unies en matière de cybersécurité. Les entreprises connexes sont dès lors d'un intérêt limité pour le présent examen.

Axe de travail II : information et télécommunications dans le contexte de la sécurité internationale

À dater de 1998, dans le cadre de ce second axe de travail intergouvernemental, « l'examen, au niveau multilatéral, des dangers réels et des risques dans le domaine de la sécurité de l'information » a commencé à figurer dans les résolutions de l'Assemblée générale, en tant que question inscrite à l'ordre du jour, sous le titre « Les progrès de la téléinformatique dans le contexte de la sécurité internationale »[4]. Deux organes intergouvernementaux fonctionnant sous la Première Commission (Commission des questions de désarmement et de la sécurité internationale) de l'Assemblée générale ont été saisis du sujet : a) le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, composé d'un nombre limité d'experts nommés par le Secrétaire général et siégeant à titre personnel[5], et qui en est à sa sixième mouture depuis sa création en 2004[6] ; b) le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (ouvert à tous les États Membres de l'ONU et établi en 2018)[7]. Les deux groupes ont pour objectifs principaux « d'examiner la question des risques qui se posent ou qui pourraient se poser dans le domaine de la sécurité de l'information ainsi que les mesures de coopération qui pourraient être prises pour y parer »[8] et « de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États visés [dans] la présente résolution et de définir des moyens de les appliquer »[9]. Le Groupe de travail à composition non limitée et le sixième Groupe d'experts gouvernementaux ont tous deux achevé leurs travaux et adopté des rapports de consensus respectivement en mars et mai 2021[10]. Il est prévu que le nouveau Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, récemment créé pour la période 2021-2025, se penche sur le travail de son prédécesseur (créé pour la période 2019-2020) et se réunisse pour la première fois en 2021[11]. Les travaux de ces organes s'effectuent avec l'appui du Bureau des affaires de désarmement de l'ONU.

[2] Résolution 65/230 de l'Assemblée générale.
[3] Résolution 74/247 de l'Assemblée générale.
[4] Voir la résolution 53/70 de l'Assemblée générale et les résolutions qui lui ont succédé, dont la dernière en date A/RES/75/240.
[5] Voir la résolution 58/32 de l'Assemblée générale.
[6] Voir la résolution 73/226 de l'Assemblée générale.
[7] Voir la résolution 73/27 de l'Assemblée générale.
[8] Voir la résolution 58/32 de l'Assemblée générale, par. 4.
[9] Voir la résolution 73/27 de l'Assemblée générale.
[10] Voir A/75/816.
[11] Voir la résolution 75/240 de l'Assemblée générale.

Les mandats des entités des Nations Unies en matière de cybersécurité

Les mandats de fond et de coopération technique de plusieurs entités des Nations Unies touchent à certains aspects de la cybersécurité. L'UIT, par exemple, organise annuellement le Sommet mondial sur la société de l'information, principale plateforme de promotion des TIC pour le développement ; elle anime, à elle seule, la grande orientation C5 de ce Sommet, intitulée « Renforcement de la confiance et de la sécurité dans l'utilisation des TIC ». Dans ce rôle, elle travaille avec des parties prenantes clés pour aider des pays dans des tâches telles que l'adoption de stratégies de cybersécurité, la mise en place de capacités nationales de riposte aux incidents, la mise en œuvre de normes internationales de sécurité, la protection des enfants et le renforcement des capacités. Certaines des activités du Sommet sont citées dans les résolutions de l'Assemblée générale intitulées « Création d'une culture mondiale de la cybersécurité », formulées dans le cadre de la Deuxième Commission de l'Assemblée générale (Commission économique et financière)[12]. L'ONUDC, l'OMPI, le PNUD, la CNUCED, le Bureau des affaires de désarmement de l'ONU et l'AIEA figurent parmi les nombreuses entités dont les mandats comprennent une composante plus ou moins grande de cybersécurité.

Il était prévu qu'un compendium des mandats et des principales activités des entités des Nations Unies relatifs à la cybersécurité et à la cybercriminalité, établi dans le cadre du CCS, servirait à répertorier tous les moyens par lesquels, dans le cadre de leurs mandats et spécialités respectifs, ces entités avaient apporté une assistance technique et un appui à la formulation de politiques dans ce domaine au fil des années. Le compendium est toutefois resté un document interne, sa finalisation et son actualisation représentant des tâches par trop monumentales. Il fournit d'abondants éléments attestant la diversité et la fragmentation du travail que les entités effectuent en la matière au titre de leurs programmes. C'est face à cet état de choses que le Comité de haut niveau sur les programmes n'a eu de cesse d'insister sur la nécessité pour le système d'adopter une démarche coordonnée et cohérente qui tienne à la fois compte de la complémentarité et du chevauchement des mandats de toutes ses entités[13].

[12] Voir les résolutions 57/239 et 64/211 de l'Assemblée générale.

[13] Voir, par exemple : CEB/2010/HLCP-XX/CRP.7, par. 3 (en anglais) ; CEB/2010/6, par. 38 à 43 (en anglais) ; CEB/2011/HLCP-XXII/CRP.6 (en anglais) ; CEB/2014/6, par. 42 à 49 (en anglais).

Annexe II

Quelques aspects de la cybersécurité abordée sous l'angle de la gestion des risques

Les Inspecteurs souhaitent mettre en exergue des mesures qui, outre l'adjonction de la cybersécurité au registre ou à la matrice des risques d'une entité, peuvent accélérer la concrétisation des avantages de l'application de la gestion des risques à la cybersécurité : a) les évaluations des risques sont conçues sur mesure, systématiques et adaptives ; b) l'appétit pour le risque et la tolérance au risque font l'objet d'une déclaration stratégique de haut niveau ; c) les spécialistes de la cybersécurité ont des occasions suffisantes d'alimenter de leurs compétences techniques le processus de gestion des risques ; d) les tests d'intrusion sont utilisés comme outils de gestion des risques.

- **Évaluation des risques adaptée à l'entité.** Les évaluations des cyberrisques qui pèsent sur une entité doivent s'effectuer d'une manière adaptée au contexte dans lequel l'entité fonctionne, compte dûment tenu de critères tels que son mandat, ses ressources financières et humaines, son modèle d'activité, le type d'informations dont elle est dépositaire ou propriétaire, et ses particularités institutionnelles, notamment la façon dont une atteinte à sa cybersécurité affecterait l'exécution des tâches relevant de son mandat, y compris en ses implantations décentralisées ou en ses diverses activités sur le terrain. Certaines entités disent fonder leurs processus d'évaluation des risques sur des normes sectorielles, ce qui peut être considéré comme une bonne pratique, pour autant que les normes elles-mêmes soient sélectionnées sur la base de leur adéquation au contexte de l'entité concernée (par. 59 à 64). Outre qu'elles doivent être adaptées à l'entité, les évaluations des risques doivent également s'effectuer périodiquement, de sorte à favoriser une approche systématique, mais aussi à assurer l'adaptabilité du cadre et, idéalement, sa réactivité à un paysage de menaces dont l'évolution constante risque de ne pas être en phase avec les cycles d'examen réguliers.
- **Déclaration d'appétit pour le risque et de tolérance au risque.** Un élément clé d'une approche plus stratégique de la gestion des cyberrisques est la formulation d'une déclaration d'appétit pour le risque et de tolérance au risque, idéalement avec la participation des organes délibérant et directeur de l'entité, ainsi que de sa direction exécutive (par. 53 et 54). Pour être la plus utile possible, cette déclaration sera fondée sur une évaluation complète et périodique des cyberrisques, couvrant toutes les catégories de menaces à la cybersécurité, sans se limiter à celles qui sont le fait d'adversaires ou qui trouvent leur origine à l'extérieur de l'entité (par. 25 à 29), ainsi que sur les informations provenant du service des TIC concernant l'état des systèmes informatiques institutionnels et les vulnérabilités connues, et des unités administratives dans l'esprit d'une approche à l'échelle de l'entité dans sa totalité. La détermination du juste niveau d'appétit pour le risque acquiert une importance cruciale lorsqu'elle se fonde sur un ensemble d'indicateurs de cybersécurité significatifs soigneusement sélectionnés et conçus. Il s'agit d'un processus propre à l'entité qui conditionnera les décisions de gestion, telles que la mise en place de capacités de cybersécurité institutionnelles internes (au lieu de recourir à des services externes), les ressources à leur consacrer, les instruments et les orientations à inclure dans le cadre réglementaire, et les décisions relatives aux investissements et aux ripostes en cas d'aggravation. Dans des entités telles que l'OMPI et l'AIEA, qui gèrent des informations particulièrement sensibles, l'appétit pour le risque peut être faible d'entrée de jeu. Une exposition antérieure à d'importantes atteintes à la cybersécurité peut également réduire l'appétit pour le risque d'une entité, avec le danger qu'un surinvestissement dans les cyberdéfenses peut donner lieu à un sentiment trompeur de sécurité.

- **Apport de compétences spécialisées en cybersécurité dans les processus de gestion des risques**. Il peut sembler évident que des compétences spécialisées en cybersécurité viennent éclairer les processus de gestion du risque institutionnel. C'est pourtant loin d'être le cas dans de nombreuses entités. Le format et la périodicité de cet apport ne sont pas décisifs, mais il est essentiel que les spécialistes de la cybersécurité aient un accès fiable (non entravé et non ponctuel) aux mécanismes moteurs de la gestion des risques au sein de l'entité. Cet accès devrait avoir un caractère systématique de sorte que les considérations de cybersécurité soient incluses dans les phases de conception, de mise en œuvre et de surveillance du cadre de gestion du risque institutionnel. Dans certaines entités où ce poste existe, le responsable de la sécurité de l'information prend part aux activités du comité de gestion du risque institutionnel ou en est un membre à part entière. Les retours d'information concernant ces dispositions étaient positifs. Il pourrait être avantageux d'en faire une pratique pour toutes les entités.

- **Tests d'intrusion en tant qu'outils de gestion des risques.** Le test d'intrusion (*penetration testing* ou *pen testing*) est la simulation autorisée d'une attaque telle qu'il en existe vraiment, visant les réseaux, les systèmes et les ressources humaines des entités. Les moyens et techniques employés à cette fin sont ceux qu'utilisent les attaquants et le but est de détecter d'éventuelles vulnérabilités dans les protections d'une entité, d'évaluer l'efficacité des mesures d'atténuation mises en place et de mettre à l'épreuve les procédures de riposte et de reprise. Les tests d'intrusion sont effectués le plus souvent par des prestataires de services externes selon des règles conçues pour permettre une évaluation adaptée et utile tout en réduisant au minimum le danger auquel l'exercice peut exposer les actifs et les processus des entités. Plusieurs entités participantes utilisent cet outil, recourant parfois à différents prestataires, aux profils variés de préférence, au cours d'une période donnée (en les faisant alterner, par exemple). Le prestataire a pour tâche d'attaquer l'entité (équipe rouge ou *red team*) et de mettre à l'épreuve l'état de préparation des défenses (équipe bleue ou *blue team*). Aux fins de cet exercice, une entité a choisi de réunir le personnel du prestataire externe (chargé de simuler l'attaque) et les membres de son centre des opérations de sécurité (chargés de la défendre contre l'attaque) pour que les deux équipes puissent communiquer en temps réel concernant les résultats et les mesures d'atténuation possibles (équipe violette ou *purple team*). Qu'ils soient effectués par un ou plusieurs prestataires externes, les tests d'intrusion sont une activité exigeante qui demande une bonne préparation et la sélection d'évaluateurs spécialisés dignes de confiance (jouant le rôle d'attaquants), car les risques sont réels lorsque l'on permet à des tiers d'accéder, même temporairement, à des systèmes et des informations sensibles. Cela étant, il s'agit d'un outil de gestion des risques perfectionné et efficace qui peut aider à planifier la continuité des opérations et qui est un moyen éprouvé de se faire une idée du dispositif de cybersécurité d'une entité sous divers angles, en mettant en évidence des lacunes dans ses défenses générales ou certaines vulnérabilités dans tel ou tel domaine particulier, selon la portée prédéfinie de l'exercice.

Annexe III

Les principales normes relatives à la cybersécurité utilisées par les entités participantes du Corps commun d'inspection

La norme ISO 27001 (Organisation internationale de normalisation, 2005)[1]

Principalement utilisée à des fins d'audit et de conformité, la norme ISO 27001 porte et informe avant tout sur les exigences techniques auxquelles doivent répondre les défenses de cybersécurité. La norme comporte 14 séries d'objectifs et de mesures de référence relatifs à l'intégration de la cybersécurité dans les objectifs opérationnels et dans les pratiques de gestion des risques d'une organisation. Les principales séries portent sur les politiques de sécurité de l'information, la gestion des actifs, le contrôle de l'accès, la sécurité liée à l'exploitation et aux communications, la gestion des incidents et la conformité. Compte tenu de ses caractéristiques, ce cadre semble plus adapté aux examens et aux audits des mesures de cybersécurité des entités d'une certaine taille dotées de ressources suffisantes.

Le cadre du National Institute of Standards and Technology (États-Unis), 1901[2]

En partant de la définition des objectifs et des priorités de l'organisation et de l'organisation des actions appropriées, l'Institut fournit des consignes flexibles et adaptables pour comprendre les cyberrisques. Outre ses consignes propres, le cadre, dont la dernière mise à jour date de 2015, comprend également des renvois à d'autres normes, consignes et pratiques, notamment les mesures de contrôle du Center for Internet Security, les normes internationales de l'ISO, les Objectifs de contrôle de l'information et des technologies associées, et d'autres. Le plan d'action de l'Institut énonce cinq fonctions centrales (définir, protéger, détecter, riposter et rétablir) et classe les flux d'information et de décisions en différents niveaux au sein de l'organisation. Par la globalité de son approche, cette norme semble convenir particulièrement bien pour définir les stratégies et règles de cybersécurité d'une organisation.

Les Objectifs de contrôle de l'information et des technologies associées (Association de l'audit et du contrôle des systèmes d'information (ISACA), 1996)[3]

Les Objectifs de contrôle constituent un cadre de gouvernance et de gestion des technologies de l'information fondé sur les meilleures pratiques qui aident les organisations à réaliser leurs objectifs dans les domaines de la conformité et de la gestion des risques, et à accorder leur stratégie en matière de technologies de l'information avec leurs objectifs. Fondée sur la notion de niveaux de capacités, cette approche met l'accent sur l'adaptation des services aux besoins de l'organisation. Conformément à cette norme internationale, des éléments de la sécurité de l'information sont inclus dans la gestion des risques ainsi que dans les mesures de continuité et de disponibilité des services opérationnels. Outre leur propre documentation, les Objectifs de contrôle renvoient à d'autres normes et guides, dont le cadre du National Institute of Standards and Technology (États-Unis), la norme ISO 27001 et les mesures de contrôle du Center for Internet Security. Les objectifs d'alignement les plus pertinents contenus dans les Objectifs de contrôle sont la gestion des risques relatifs aux technologies de l'information, la sécurité de l'information, la conformité, ainsi que la continuité et la disponibilité des services opérationnels. En ce qui concerne les consignes relatives à la cybersécurité, la norme semble particulièrement bien adaptée aux organisations qui utilisent déjà les Objectifs de contrôle pour la gouvernance et la gestion de leurs TIC. Ses critères peuvent en outre être étendus par combinaison avec les autres normes auxquelles elle renvoie (les mesures du Center for Internet Security Controls, le cadre du National Institute of Standards and Technology (États-Unis) et la norme ISO 27001).

[1] Disponible à l'adresse www.iso.org/fr/hom e.html.
[2] Disponible à l'adresse www.ist.gov/ (en anglais).
[3] Disponible à l'adresse www.isaca.org/credentialing/cobit/cobit-foundation (en anglais).

Les directives de la Information Technology Infrastructure Library (Central Computer and Telecommunications Agency (Royaume-Uni), années 1980)[4]

La Information Technology Infrastructure Library, ou bibliothèque pour l'infrastructure des technologies de l'information, est constituée de directives pour la gestion des services informatiques, qui sont présentées sous la forme d'une série de publications fournissant des consignes pour la prestation des services informatiques et pour la mise en place des processus et des ressources nécessaires à cette fin. Mise au point par la Central Computer and Telecommunications Agency (Royaume-Uni) au cours des années 1980, cette norme est constituée de cinq volumes, chacun consacré à une phase différente du cycle de gestion des services informatiques : valeur des services, développement des services, actifs des services, analyse de marché et types de prestataires. Depuis 2005, les pratiques de la bibliothèque contribuent à la norme ISO 20000 et sont alignées sur elle.

Les mesures de contrôle du Center for Internet Security, 2008[5]

Sous les appellations Center for Internet Security Controls ou Critical Cybersecurity Controls, cette norme fournit une série de recommandations fondées sur les meilleures pratiques du secteur. Bien que l'orientation soit avant tout technique, quelques mesures de contrôle portent sur certains aspects assez larges de la cybersécurité, comme la sensibilisation et la riposte aux incidents. Le cadre se présente sous un jour assez pratique et très utile, en ce qu'il met l'accent sur son application en fonction de la taille, des compétences, des ressources disponibles et de la nature plus ou moins sensible des données de l'organisation. Ses principales mesures de contrôle portent sur l'inventaire et les actifs, la gestion des vulnérabilités, la configuration dans de bonnes conditions de sécurité, la protection des messageries et des navigateurs du Web, la récupération et la protection des données, la riposte aux incidents, et les tests d'intrusion. Cette approche s'est avérée particulièrement bien adaptée à la mise en œuvre de stratégies de cyberdéfense dans les petites et moyennes organisations qui disposent déjà de cadres de gestion des risques comprenant des éléments de cybersécurité.

[4] Disponible à l'adresse www.axelos.com/best-practice-solutions/itil.
[5] Disponible à l'adresse www.cisecurity.org/controls/.

Annexe IV

Les cadres réglementaires des entités des Nations Unies en matière de cybersécurité

a) Les niveaux du cadre réglementaire de la cybersécurité

Niveau stratégique	Souvent un seul document contenant des déclarations de haut niveau formulées en termes d'aspirations	Définit le projet, les objectifs et les principes fondamentaux au niveau de l'entité ; énonce les rôles et les responsabilités aux niveaux de la gouvernance et des opérations ; peut présenter la cybersécurité comme une décision de gestion, assortie d'une déclaration de la tolérance au risque ou de l'appétit pour le risque de l'entité	S'applique au niveau institutionnel de l'entité et s'adresse principalement à l'équipe de direction, responsable de sa mise en œuvre
Niveau des règles	Une série de documents autonomes formulés en termes normatifs et applicables, habituellement publiés sous forme de textes administratifs officiels	Formulent les principes institutionnels qui sous-tendent le système de gestion de la sécurité de l'information, assortis de règlements et de règles intérieurs contraignants, exposant les objets et les actions correspondantes, agencés par sujet (par exemple, classification de l'information, gestion des risques, continuité des opérations, reprise après sinistre et utilisation acceptable des données et actifs informatiques et de communication), et attribuent les rôles et les responsabilités	S'appliquent à tous les membres du personnel et supposent l'imposition éventuelle de sanctions disciplinaires en cas de non-respect
Niveau des procédures	Une série de directives ou d'instructions permanentes appuyant les politiques arrêtées à un niveau supérieur en décrivant les processus visant à établir des pratiques systématiques	Fournissent des consignes détaillées sur les mesures à prendre ou les comportements à éviter (respect des conventions relatives à l'utilisation des mots de passe, effectuer régulièrement des analyses antivirus et des mises à jour des logiciels, scanner avant usage les bus sériels universels (USB) offerts, etc.)	Peuvent s'appliquer à tous les membres du personnel ou viser certains rôles (par exemple, le personnel des services des TIC, les responsables des archives et des dossiers, les spécialistes des acquisitions)
Niveau technique	Une série de protocoles techniques visant une exécution correcte et uniforme	Fournissent des instructions détaillées, étape par étape, dont l'application requiert un niveau élevé de savoir-faire spécialisé, couvrant des sujets tels que la configuration des bases de données, la sécurité des réseaux et la sécurité de l'informatique en *cloud* (ou en nuage)	S'adressent principalement aux spécialistes techniques

Source : Établi par le CCI.

b) Stratégies relatives aux technologies de l'information et des communications et documents d'orientation visant spécifiquement la cybersécurité dans les entités participantes

Entité participante	*Stratégie institutionnelle des technologies de l'information et des communications comprenant la cybersécurité*	*Documents d'orientation visant spécifiquement la cybersécurité*
Secrétariat de l'ONU	Oui, Informatique et communications à l'Organisation des Nations Unies (A/69/517) et résolution 69/262 de l'Assemblée générale	Oui, directive relative à la politique de sécurité de l'information pour le Secrétariat de l'ONU (*Information Security Policy Directive for the United Nations Secretariat*) (2013)
CNUCED	Suit la stratégie du Secrétariat de l'ONU relative à l'informatique et aux communications	Oui, suit la stratégie du Secrétariat de l'ONU relative à la cybersécurité
FNUAP	Oui, stratégie relative aux technologies de l'information et des communications (*Information and Communications Technology Strategy*) (2018-2021)	Oui, politique relative à la sécurité des technologies de l'information et des communications (*Information and Communications Technology Security Policy*)
HCR	Oui, stratégie relative aux technologies de l'information (*Information Technology Strategy*) (2020-2022) (projet final en cours d'examen)	En cours d'élaboration
ONUDC/ONUV	Suit la stratégie du Secrétariat de l'ONU relative à l'informatique et aux communications	Oui, suit la stratégie du Secrétariat de l'ONU relative à la cybersécurité
ONU-Femmes	Oui, stratégie relative aux technologies de l'information et des communications (*Information and Communication Technologies Strategy*) (2018-2021)	Oui, politique relative à la sécurité de l'information (*Information Security Policy*)
ONU-Habitat	Suit la stratégie du Secrétariat de l'ONU relative à l'informatique et aux communications	Oui, suit la stratégie du Secrétariat de l'ONU relative à la cybersécurité
ONUSIDA	Non, la stratégie relative aux TIC (*ICT Strategy*) (2017-2020) ne comprend pas la cybersécurité	Non, ONUSIDA élabore un plan global relatif à la cybersécurité qui comprendra une politique relative à la cybersécurité
PAM	Oui, stratégie institutionnelle relative aux technologies de l'information (*Corporate Information Technology Strategy*) (2016-2020)	Oui, politique institutionnelle relative à la sécurité de l'information et des technologies de l'information (*Corporate Information and Information Technology Security Policy*) (2015)
PNUD	Oui, stratégie des technologies de l'information (*Information Technology Strategy*) (2020-2023)	Oui, politique relative à la sécurité de l'information (*Information Security Policy*) (2016)
PNUE	Suit la stratégie du Secrétariat de l'ONU relative à l'informatique et aux communications	Oui, suit la stratégie du Secrétariat de l'ONU relative à la cybersécurité
UNICEF	Oui, stratégie des technologies de l'information et des communications (*Information and Communication Technologies Strategy*)	Oui, le plan stratégique pour la sécurité de l'information (*UNICEF Information Security Strategic Plan*) (2018-2022)

Entité participante	*Stratégie institutionnelle des technologies de l'information et des communications comprenant la cybersécurité*	*Documents d'orientation visant spécifiquement la cybersécurité*
UNOPS	Une stratégie quinquennale relative aux TIC est en cours d'élaboration	Oui, sécurité de l'information (*Information Security*)
UNRWA	Oui, stratégie du département de gestion de l'information (*Information Management Department Strategy*) (2019-2020)	Il existe une politique distincte relative à la sécurité de l'information (en attente d'approbation finale)
AIEA	Oui, plan stratégique relatif aux technologies opérationnelles (*Business Technology Strategic Plan*) (2015-2020)	Oui, normes relatives à la sécurité de l'information (*Standards on Information Security*)
BIT	Oui, stratégie relative aux technologies de l'information (*Information Technology Strategy*) (2018-2021)	Oui, déclarations de politique générale relatives à la sécurité de l'information électronique (*Electronic Information Security Policy Statements*) (2010)
FAO	Oui, stratégie numérique relative aux technologies de l'information et des communications (*Information and Communication Technologies Digital Strategy*) (2017)	Oui, politique relative à la sécurité de l'information (*Information Security Policy*)
OACI	Oui, stratégie numérique relative aux technologies de l'information et des communications (*Information and Communication Technologies Digital Strategy*) (2017) (en cours de réexamen)	Oui, politique relative à la sécurité de l'information (*Information Security Policy*) (2007, Rév. 2)
OMI	Oui, plan stratégique relatif aux technologies de l'information et des communications (*Information and Communication Technologies Strategic Plan*) (2019-2023)	Oui, gestion des risques relatifs à la sécurité de l'information (*Information Security Risk Management*) (2015)
OMM	Oui, stratégie des technologies de l'information et des communications (*Information and Communication Technology Strategy*) (2020-2023)	Non
OMPI	Oui, stratégie des technologies de l'information et des communications (*Information and Communication Technologies Strategy*) (nouvelle stratégie en cours d'élaboration)	Oui, politiques et normes relatives à la sécurité de l'information (*Information Security Policies and Standards*) et stratégie relative à la sécurité de l'information de nouvelle génération (*Next Generation Information Security Strategy*) (2021-2024)
OMS	Oui, stratégie relative à la gestion et aux technologies de l'information (*Information Management and Technology Strategy*) (2019)	Oui, stratégie relative à la cybersécurité (*Cybersecurity Strategy*)
OMT	Non, la stratégie relative aux technologies de l'information et des communications (*Information and Communication Technologies Strategy*) ne comprend pas la cybersécurité	Non, en cours d'élaboration

Entité participante	*Stratégie institutionnelle des technologies de l'information et des communications comprenant la cybersécurité*	*Documents d'orientation visant spécifiquement la cybersécurité*
ONUDI	Stratégie institutionnelle relative aux technologies de l'information et des communications (*Corporate Information and Communication Technologies Strategy*) (2019-2021)	Non
UIT	Non, l'UIT adopte une démarche plus globale avec son système de gestion de la résilience institutionnelle fondé sur une analyse d'impact détaillée dans laquelle interviennent les risques stratégiques, les stratégies relatives à l'impact sur les activités, la gestion des crises, la continuité des activités et la reprise après sinistre en matière de TIC	Non
UNESCO	Oui, stratégie relative à la gestion des connaissances et aux technologies de l'information et des communications (*Knowledge Management and Information and Communication Technologies Strategy*) (2018-2021)	Oui, la cybersécurité figure dans le cadre de gestion du risque institutionnel et dans la partie du Manuel administratif consacrée à la politique de sécurité de l'information et des technologies de l'information (*Information and Information Technology Security Policy*)
UPU	Non, la stratégie relative aux TIC sera disponible en décembre 2021	Non

Annexe V

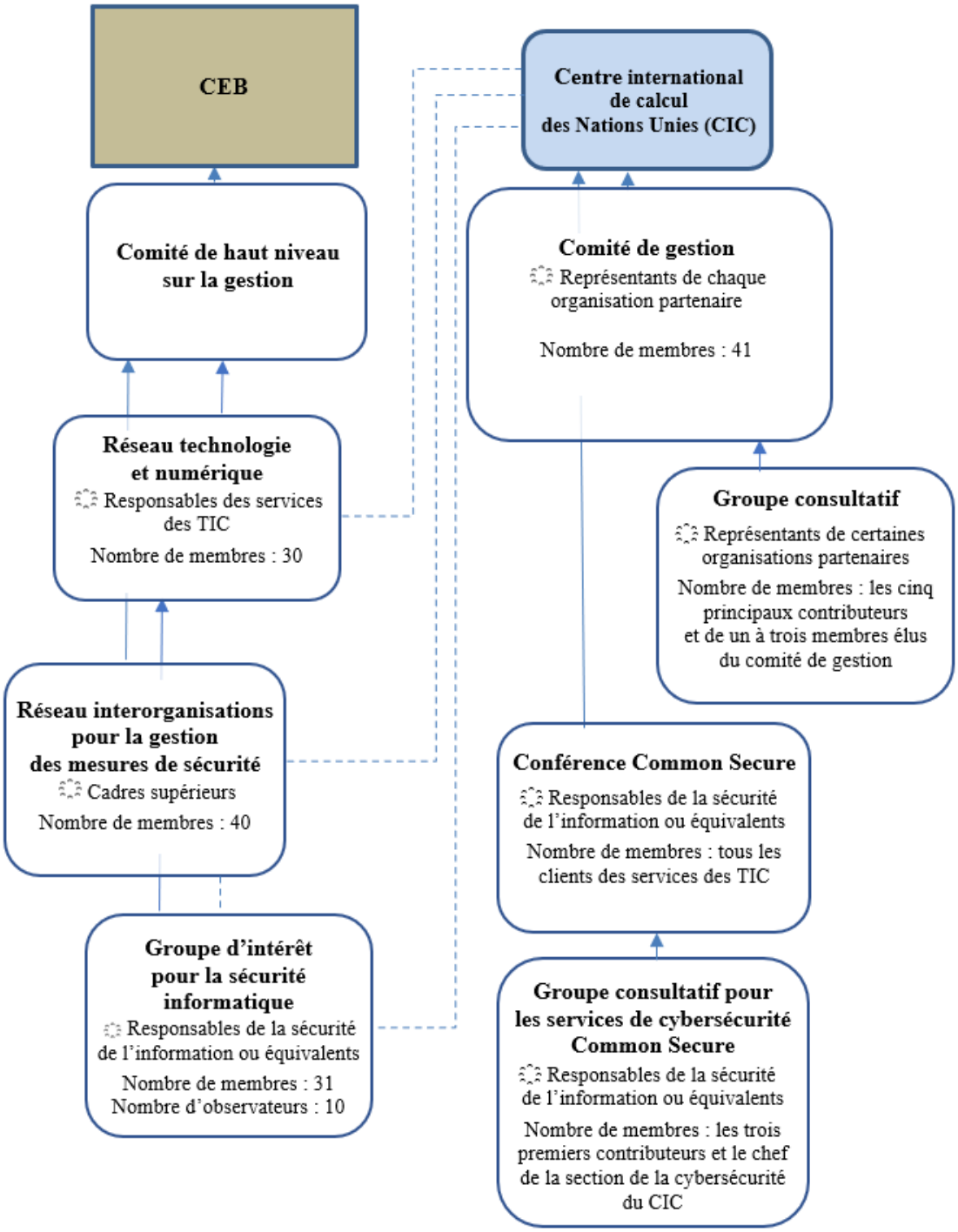
Les structures administratives chargées de la cybersécurité et leurs rattachements hiérarchiques au sein des entités participantes du Corps commun d'inspection (janvier 2021)

Entités participantes	*Les questions de cybersécurité sont gérées par des capacités internes spéciales ou spécialisées*	*La cybersécurité relève du service institutionnel des TIC (au même titre que les autres fonctions relatives aux TIC)*	*L'entité a utilisé le service de gouvernance de la sécurité (« responsable de la sécurité de l'information en tant que service ») fourni par le Centre international de calcul des Nations Unies*	*Rattachement direct au chef du service des TIC*
Secrétariat de l'ONU	√		X	√
CNUCED		√	√ (Cliente actuelle)	√
FNUAP	√ (Responsable de la sécurité de l'information en cours de recrutement)	√ (En attendant l'aboutissement de la procédure de recrutement)	√ (Client actuel)	√
HCR	√		X	√
ONUDC/ONUV		√	X	√
ONU-Femmes		√	√ (Ancienne cliente)	√
ONUSIDA		√	X	√
PAM	√		√ (Ancien client)	√
PNUD	√		X	√
PNUE		√	X	√
UNICEF	√		√ (client actuel)	√
UNOPS	√		X	Le responsable de la sécurité de l'information est placé sous l'autorité du responsable du service financier et du Directeur de l'administration
UNRWA	√		X	√
AIEA	√		X	√
BIT	√		X	√
FAO	√		√ (Ancienne cliente)	√

Entités participantes	*Les questions de cybersécurité sont gérées par des capacités internes spéciales ou spécialisées*	*La cybersécurité relève du service institutionnel des TIC (au même titre que les autres fonctions relatives aux TIC)*	*L'entité a utilisé le service de gouvernance de la sécurité (« responsable de la sécurité de l'information en tant que service ») fourni par le Centre international de calcul des Nations Unies*	*Rattachement direct au chef du service des TIC*
OACI	√		√ (Ancienne cliente)	Le responsable de la sécurité de l'information est placé sous l'autorité directe du directeur de l'administration
OMI		√	**X**	√
OMM		√	√ (Cliente actuelle)	√
OMPI	√		**X**	Responsable à la fois de la sécurité physique et de la sécurité de l'information, le Directeur de la Division de la sécurité et de l'assurance informatique a pour supérieur hiérarchique le Sous-Directeur général chargé du Secteur administration, finances et gestion
OMS	√		√ (Ancienne cliente)	√
OMT		√	**X**	√
ONUDI		√	**X**	√
UIT	√		**X**	√
UNESCO	√		√ (Cliente actuelle)	√
UPU		√	**X**	√

Annexe VI

Les dispositions interentités d'ordre institutionnel concernant la cybersécurité



Source : Établi par le CCI.

Annexe VII

Récapitulatif des services du Centre international de calcul des Nations Unies utilisés par des entités participantes du Corps commun d'inspection (janvier 2021)

Services de cybersécurité	*Brève description*	*Nombre d'entités participantes du Corps commun d'inspection actuellement abonnées*	*Nombre d'entités participantes du Corps commun d'inspection précédemment abonnées*
Renseignements Common Secure sur les menaces (*Common Secure threat intelligence*)	Collecte des informations en continu et en temps utile auprès de membres, d'entreprises de sécurité commerciales, de prestataires de services, d'autorités nationales et territoriales, de services de police et de justice, et d'autres sources de confiance, qui permet aux entités abonnées de partager tous renseignements pertinents et utiles concernant les menaces et les atteintes à la cybersécurité.	17	
Service commun de signature électronique (*Common e-Signature service*)	Met à disposition une solution de signature numérique.	14	
Sensibilisation à la sécurité de l'information (*Information security awareness*)	Fournit des conseils stratégiques pour la mise sur pied de stratégies avancées et efficaces de sensibilisation à la sécurité de l'information, un laboratoire de pointe en *cloud* (ou en nuage) pour l'apprentissage et des supports de communication, notamment des produits à messages, des bulletins, des affiches et un soutien par portail.	7	3
Gestion des vulnérabilités (*Vulnerability management*)	Combinaison de processus et de technologies pour la détection et la résolution en continu des vulnérabilités et des vices de configuration, notamment par l'analyse des vulnérabilités des serveurs et des applications, la vérification des configurations de sécurité et la surveillance de l'empreinte numérique.	6	1
Services de gouvernance et d'appui aux responsables de la sécurité de l'information (*Governance and chief information officer support services*)	Services du système de gestion de la sécurité de l'information visant à protéger les actifs institutionnels et à atténuer les risques d'atteinte à la réputation, de perte d'information, d'exposition à des actes malveillants, de violation des droits de propriété intellectuelle et de compromission des données sensibles.	6	5

Services de cybersécurité	*Brève description*	*Nombre d'entités participantes du Corps commun d'inspection actuellement abonnées*	*Nombre d'entités participantes du Corps commun d'inspection précédemment abonnées*
Services de simulation d'hameçonnage (*Phishing simulation services*)	Mettent à l'épreuve l'efficacité des programmes de sensibilisation à la sécurité de l'information exécutés par entités, par la conception, l'exécution et le suivi de campagnes de simulation d'hameçonnage.	6	
Centre commun des opérations de sécurité (*Common security operations centre service*)	Met à disposition des compétences spécialisées pour surveiller, analyser et gérer les faits de cybersécurité, et donner aux entités abonnées les moyens de riposter en temps utile aux atteintes à la cybersécurité, par la mise en œuvre d'une combinaison de processus et de solutions technologiques.	4	1
Intervention en cas d'incident (*Incident response*)	Met à disposition des procédures de gestion des incidents conformes aux normes sectorielles pour analyser les données relatives aux atteintes et déterminer les ripostes appropriées en temps réel.	4	7
Évaluation de la sécurité de l'information en *cloud* (*Cloud security assessment*)	Évaluation, migration, mise en œuvre, soutien opérationnel pleinement géré et gestion des coûts pour plusieurs solutions d'informatique en *cloud* (ou en nuage).	4	1
Test d'intrusion (*Penetration testing*)	Repère les faiblesses dans les mesures de contrôle de la sécurité de l'information et détermine la mesure dans laquelle des adversaires peuvent pénétrer dans le réseau ou les systèmes testés.	3	4
Infrastructure commune à clés publiques (*Common public key infrastructure*)	Des clés publiques et privées d'encodage et des signatures numériques sont fournies et gérées en vue de créer un environnement sûr pour les transactions électroniques et les transferts de données.	3	
Gestion des identités et des accès (*Identity and access management*)	Collecte, analyse et présentation d'informations sur les applications de gestion des identités et des accès.	2	1
Gestion commune des informations et des événements de sécurité (*Common security information and event management*)	Analyse en temps réel les alertes de sécurité générées par les applications et les matériels en réseau.	1	

Source : Catalogue de services du Centre international de calcul des Nations Unies (juillet 2021) et réponses des entités participantes au questionnaire du CCI.

Annexe VIII

Tableau comparatif de l'état des adhésions aux entités chargées de questions de cybersécurité (janvier 2021)

Entités participantes	*Réseau Technologie et numérique (trente-troisième session, 2019)*	*Groupe d'intérêt pour la sécurité informatique (huitième symposium, 2019)*	*Centre international de calcul des Nations Unies Comité de gestion (2020)*	*Centre international de calcul des Nations Unies Clients passés et actuels*
Secrétariat de l'ONU	√	√	√	X
CNUCED	√	X	√	√
FNUAP	√	√	√	√
HCR	√	√	√	√
ONUDC/ONUV	X	X	X[1]	√
ONU-Femmes	√	√	√	√
ONU-Habitat	√	X	X[2]	X
ONUSIDA	√	X	√	X
PAM	√	√	√	√
PNUD	√	√	√	√
PNUE	√	X	√	X
UNICEF	√	√	√	√
UNOPS	√	X	√	√
UNRWA	√	X	√	√
AIEA	√	√	√	√
BIT	√	√	√	√
FAO	√	X	√	√
OACI	√	X	√	√
OMI	√	X	√	√
OMM	√	√	√	√
OMPI	√	√	√	√
OMS	X	√	√	√
OMT	X	√	X	√
ONUDI	√	√	√	√

[1] Le Centre de calcul international des Nations Unies a signalé que l'ONUDC/l'Office des Nations Unies à Vienne étaient représentés au comité de gestion par le Secrétariat de l'ONU.

[2] Le Centre de calcul international des Nations Unies a signalé qu'ONU-Habitat était représenté au comité de gestion par le Secrétariat de l'ONU.

Entités participantes	*Réseau Technologie et numérique (trente-troisième session, 2019)*	*Groupe d'intérêt pour la sécurité informatique (huitième symposium, 2019)*	*Centre international de calcul des Nations Unies Comité de gestion (2020)*	*Centre international de calcul des Nations Unies Clients passés et actuels*
UIT	√	√	√	√
UNESCO	√	**X**	√	√
UPU	**X**	√	√	**X**

Annexe IX

Glossaire de termes relatifs à la cybersécurité

Réseau de zombies (*botnet*), gestion de réseau de zombies (*bot herding*)	Un réseau de zombies ou *botnet* est constitué d'un grand nombre d'ordinateurs compromis utilisés pour créer et envoyer du pourriel (*spam*) ou des virus, ou pour inonder un réseau de messages dans le cadre d'une attaque par déni de service. *Source* : ESCAL Institute of Advanced Technologies, *Glossary of Security Terms* www.sans.org/security-resources/glossary-of-terms/
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril la confidentialité, l'intégrité ou la disponibilité de ladite information. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Attaque par déni de service distribué	Attaque par laquelle une multitude de systèmes compromis visent une même cible. Le flux de messages envoyés est tel qu'il provoque une panne du système ciblé et l'interruption des services offerts aux utilisateurs légitimes. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Encodage, chiffrement, cryptage	Une fonction mathématique qui protège une information en la rendant illisible à tout utilisateur qui ne dispose pas de la clé de décodage. *Source* : National Cyber Security Centre (Royaume-Uni) www.ncsc.gov.uk/information/ncsc-glossary
Appareil final	Tout appareil connecté à un réseau, tel qu'un ordinateur de bureau, un ordinateur portable, un smartphone, une tablette, une imprimante ou tout autre matériel, comme un terminal de point de vente ou un kiosque de vente au détail, qui sert de point d'extrémité pour l'utilisateur dans un réseau distribué. *Source* : Barracuda Networks Inc., *Glossary* www.barracuda.com/glossary/endpoint-device
Coupe-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre. Les ressources du système local sont ainsi protégées contre un accès de l'extérieur. (Synonyme : pare-feu.) *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Internet des objets	Réseau formé par les dispositifs Web utilisés couramment, qui peuvent se connecter les uns aux autres et qui peuvent se transmettre de l'information. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire

Hameçonnage (*phishing*)	Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les mystifiant ou en imitant une marque commerciale connue dans le but de réaliser des gains financiers. En l'occurrence, les malfaiteurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de carte de crédit, informations bancaires ou autres renseignements) afin de s'en servir pour commettre des actes frauduleux. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Rançongiciel (*Ransomware)*	Type de maliciel qui empêche tout utilisateur légitime d'accéder à des ressources (système ou données), et ce, jusqu'à ce que les responsables desdites ressources aient payé une rançon. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Informatique fantôme (*Shadow IT)*	Utilisation de matériels ou de logiciels par un service ou par un individu à l'insu du service d'informatique ou du service de sécurité de son organisation. *Source* : Cisco www.cisco.com/c/en/us/products/security/what-is-shadow-it.html
Piratage psychologique	Procédé de manipulation, aussi appelé « ingénierie sociale », par lequel une personne est amenée à effectuer certains actes ou à révéler certaines informations dont un attaquant pourra tirer profit. *Source* : National Cyber Security Centre (Royaume-Uni) www.ncsc.gov.uk/information/ncsc-glossary
Harponnage (*spear phishing)*	Utilisation de courriels trompeurs dans le but de persuader des membres d'une organisation de révéler leurs noms d'utilisateurs et leurs mots de passe. Contrairement à l'hameçonnage, qui nécessite l'envoi massif de courriels, le harponnage se fait à petite échelle et est bien ciblé. (Synonyme : hameçonnage ciblé.) *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Usurpation d'adresse (*Spoofing*)	Simuler l'adresse d'expédition d'une transmission électronique afin d'accéder illégalement à un système sécurisé. *Source* : Committee on National Security Systems (États-Unis) https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
Réseau privé virtuel	Réseau de communication privé habituellement utilisé au sein d'une entreprise ou par plusieurs entreprises pour communiquer au moyen d'un réseau plus vaste. Les communications par RPV sont habituellement chiffrées ou encodées pour en protéger le trafic contre les utilisateurs du réseau public qui sert de support au RPV en question. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens ou les activités d'une organisation. *Source* : Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire

Annexe X

Vue d'ensemble des mesures que les entités participantes sont appelées à prendre conformément aux recommandations du Corps commun d'inspection

		Effet escompté	*Organisation des Nations Unies, ses fonds et ses programmes*																*Institutions spécialisées et AIEA*												
			CCI	*Nations Unies*	*ONUSIDA*	*CNUCED*	*ITC*	*PNUD*	*PNUE*	*FNUAP*	*ONU-Habitat*	*HCR*	*UNICEF*	*ONUDC*	*UNOPS*	*UNRWA*	*ONU-Femmes*	*PAM*	*FAO*	*AIEA*	*OACI*	*BIT*	*OMI*	*UIT*	*UNESCO*	*ONUDI*	*OMT*	*UPU*	*OMS*	*OMPI*	*OMM*
Rapport	Pour suite à donner		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Pour information		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Recommandation 1		**f**		**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**
Recommandation 2		**f**		**L**	**L**			**L**	**L**	**L**			**L**		**L**		**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
Recommandation 3		**c**	**E**																												
Recommandation 4		**c**		**L**																											
Recommandation 5		**f**		**E**																											

Légende :

L : Recommandation appelant une décision de l'organe délibérant.

E : Recommandation au chef de secrétariat pour suite à donner.

☐ : La recommandation n'appelle pas de mesure de la part de cette entité.

Effet escompté : a : transparence et responsabilisation renforcées ; **b :** diffusion de bonnes/meilleures pratiques ; **c :** coordination et coopération renforcées ; **d :** cohérence et harmonisation renforcées ; **e :** contrôle et conformité renforcés ; **f :** efficacité renforcée ; **g :** économies importantes ; **h :** efficience renforcée ; **i :** autres.