Nations Unies A/77/88/Add.1

Assemblée générale

Distr. générale
7 juin 2022
Français
Original : anglais

Soixante-dix-septième session
Point 145 de la liste préliminaire*
Corps commun d'inspection

Examen de la cybersécurité dans les entités des Nations Unies

Note du Secrétaire général

Le Secrétaire général a l'honneur de communiquer aux membres de l'Assemblée générale ses observations et celles du Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination sur le rapport du Corps commun d'inspection intitulé « La cybersécurité dans les entités des Nations Unies » (voir A/77/88).

* A/77/50.

22-08682 (F) 160622 220622

I. Introduction

1. Dans son rapport intitulé « La cybersécurité dans les entités des Nations Unies » (voir A/77/88), le Corps commun d'inspection présente ses travaux d'examen de la cybersécurité dans les entités des Nations Unies, dont les principaux objectifs 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).

II. Observations d'ordre général

2. Les entités se félicitent du rapport et de ses conclusions, qui sont susceptibles de renforcer le dispositif de cybersécurité du système des Nations Unies. Elles apprécient en outre le fait que l'examen effectué aille dans le sens : a) d'une approche fondée sur les risques liés à leurs activités, qui va au-delà de celle traditionnellement centrée sur les technologies de l'information et des communications (TIC) ; b) d'un point de vue et de processus internes à chaque entité ; c) d'un soutien appuyé en faveur d'un niveau minimum commun de moyens de protection et de mesures de sécurité dans l'ensemble du système des Nations Unies, visant à combler l'écart de maturité entre les entités et à améliorer la cyberrésilience dans tout le système.

3. Les entités souscrivent aux recommandations issues de l'examen.

III. Observations sur les 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.

4. Les entités souscrivent à cette recommandation.

5. Dans certaines entités, il se peut que le dispositif existant de communication régulière d'informations sur la gouvernance en matière de cybersécurité réponde déjà aux besoins qui ont suscité la recommandation, par exemple moyennant l'établissement de rapports destinés aux organes directeurs, aux comités d'audit et de contrôle, aux conseils internes de ces entités en matière d'informatique et aux conseils consultatifs externes d'experts en technologie.

6. Les entités soulignent que, lors de l'établissement des rapports recommandés, il importerait de veiller à ce que ces documents publics ne contiennent aucun renseignement susceptible soit de fournir des informations précises sur la détection d'attaques et les capacités de chaque entité en la matière, soit d'être exploité par un adversaire potentiel pour augmenter la probabilité de réussite de ses attaques.

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.

7. Les entités notent que cette recommandation s'adresse à leurs organes délibérants et directeurs.

8. Les attentes en matière d'orientations stratégiques doivent tenir compte du fait qu'il faudrait des ressources supplémentaires pour renforcer le dispositif de sécurité local et faciliter la collaboration avec le Centre international de calcul des Nations Unies (CIC).

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.

9. Les entités notent que cette recommandation s'adresse au Directeur du CIC.

10. Les petites entités qui manquent de ressources et de compétences en matière de cybersécurité pourraient tirer parti des services partagés supplémentaires que le CIC élaborerait dans ce domaine. Les entités qui exécutent leurs programmes numériques de développement et d'action humanitaire dans le cadre de partenariats privé-public sont désireuses de continuer de recevoir un soutien direct des États Membres pour mener à bien ces programmes, y compris en ce qui concerne les aspects liés à leur cybersécurité. À cet égard, l'interprétation que certaines entités ont de cette recommandation est que celle-ci s'applique au dispositif de cybersécurité interne de leurs bureaux dans le monde entier ainsi qu'au dispositif de cybersécurité relatif aux activités externes menées avec des partenaires privés-publics et aux risques qui en découlent.

11. Certaines entités membres du CIC indiquent que, si cette recommandation est appliquée, elles envisagent de jouer un rôle, notamment en tant que membres du Réseau Technologie et numérique, dans les discussions concernant la gouvernance, le financement et la mise en œuvre du fonds d'affectation spéciale, ainsi que l'accès à ce fonds, avant que toute proposition soit arrêtée.

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 à ce fonds.

12. Les entités notent que cette recommandation s'adresse à l'Assemblée générale et renvoient aux observations qu'elles ont formulées au sujet de la recommandation 3.

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.

13. Les entités notent que cette recommandation s'adresse au Secrétaire général.

14. Le Secrétariat de l'ONU a déjà lancé un tel processus. Outre le fait qu'il collabore de manière informelle et ponctuelle avec le Bureau de l'informatique et des communications, le Département de la sûreté et de la sécurité est membre du réseau hybride de lutte contre les cyberattaques qui a été créé récemment. Par ailleurs, dans le cadre du plan d'équipement pour l'investissement dans le domaine de l'informatique et des communications, les investissements nécessaires seront pris en compte pour renforcer les structures, les capacités du personnel, les actifs et les services existants, en vue de tirer parti de la convergence entre sécurité physique et cybersécurité.

15. En ce qui concerne la convergence des fonctions de sécurité physique et de cybersécurité, certaines entités voient une contradiction potentielle dans le libellé du paragraphe 164 du rapport. D'une part, les inspecteurs indiquent que le groupe chargé de la sécurité physique ne doit pas absorber les fonctions de cybersécurité, d'autre part, ils préconisent la convergence de ces domaines, ce qui pourrait créer dans les différentes entités une situation susceptible de produire précisément le résultat qu'ils ne recommandent pas. Selon ces entités, il convient de souligner que les fonctions de cybersécurité ne doivent pas être absorbées par les groupes chargés de la sécurité physique.

16. Bien que le Département et le Bureau collaborent déjà sur les questions de cybersécurité, il convient de noter que ce dernier assumera la direction des opérations dans ce domaine et que le rôle et les ressources du Département seront exclusivement axés sur la sécurité physique du personnel et des locaux des Nations Unies, étant donné que la cybersécurité ne relève pas de sa compétence. Ce partenariat est activé lorsque les Nations Unies font face à des cyberattaques hybrides[1], auquel cas le Département et le Bureau collaborent pour évaluer les risques en matière de sécurité et pour formuler et appliquer des recommandations sur les mesures de prévention et d'atténuation requises.

[1] Dans ce contexte, une cyberattaque hybride s'entend d'une utilisation de la technologie numérique ou d'une attaque physique contre l'infrastructure informatique qui vise à causer un préjudice délibéré aux programmes et activités des Nations Unies et qui entraîne une grave menace pour la sécurité physique des locaux des Nations Unies ou accroît les risques auxquels sont exposés les membres du personnel.