Nations Unies A/68/7/Add.11

Assemblée générale

Distr. générale
4 décembre 2013
Français
Original : anglais

Soixante-huitième session
Point 134 de l'ordre du jour
Projet de budget-programme pour l'exercice biennal 2014-2015

État d'avancement de l'application des recommandations relatives au renforcement de la sécurité des systèmes informatiques du Secrétariat

Douzième rapport du Comité consultatif pour les questions administratives et budgétaires sur le projet de budget-programme pour l'exercice biennal 2014-2015

I. Introduction

1. Le Comité consultatif pour les questions administratives et budgétaires a examiné le rapport du Secrétaire général sur l'état d'avancement de l'application des recommandations relatives au renforcement de la sécurité des systèmes informatiques du Secrétariat (A/68/552), soumis en application de la résolution 67/254, par laquelle l'Assemblée générale a prié le Secrétaire général de faire le point, dans le projet de budget-programme pour l'exercice biennal 2014-2015, sur l'application des mesures prises pour régler les problèmes de sécurité informatique. Lors de l'examen de ce rapport, le Comité a rencontré des représentants du Secrétaire général, qui lui ont fourni des informations supplémentaires et des éclaircissements puis des réponses écrites reçues le 20 novembre 2013.

2. The Comité consultatif rappelle que dans son premier rapport sur la manière dont les questions relatives à l'informatique sont traitées au Secrétariat, y compris au Bureau de l'informatique et des communications (A/67/651), le Comité des commissaires aux comptes a indiqué que l'environnement informatique de l'Organisation des Nations Unies était insuffisamment protégé et a formulé une série de recommandations pour remédier aux faiblesses identifiées. Dans son rapport sur l'application de ces recommandations (A/67/651/Add.1), le Secrétaire général a fait savoir que le Secrétariat élaborait un plan d'action en 10 points associant des mesures à court terme pour régler les problèmes les plus urgents et la définition d'une stratégie à moyen et à long terme garantissant la sécurité informatique. Les 10 éléments du plan s'articulent selon trois axes : a) les contrôles préventifs; b) le

renforcement de la détection des incidents et des capacités d'intervention; et c) la gouvernance et la question du risque et du respect des normes.

3. Le rapport du Secrétaire général donne des informations sur la situation actuelle dans le domaine informatique, sur les premières mesures prises pour appliquer le plan d'action visant à renforcer la sécurité informatique et sur les autres mesures à prendre à cet égard. Le Secrétaire général indique qu'une stratégie de sécurité informatique complète couvrant aussi bien les sites Web que les missions sera présentée à l'Assemblée générale à sa soixante-neuvième session dans le cadre de l'examen de la stratégie de sécurité informatique globale de l'Organisation.

II. Activités exécutées à ce jour

4. Aux paragraphes 10 et 11 de son rapport, le Secrétaire général décrit les mesures prises pour appliquer le plan d'action, à savoir notamment : a) renforcement des contrôles préventifs en limitant les privilèges d'administrateur, reconfiguration des serveurs avec les nouveaux correctifs de sécurité, achat de systèmes de filtrage supplémentaires pour les sites Web et la messagerie électronique, vérification de l'infrastructure de pare-feux et remplacement par une technologie plus avancée, et achat d'un cours de formation sur ordinateur pour sensibiliser le personnel du Secrétariat au problème de la sécurité informatique; b) évaluation du degré de sécurité des applications existantes dans le cadre de l'initiative engagée afin de déterminer lesquelles seront conservées après la mise en service d'Umoja; c) acquisition d'un service géré pour le déploiement et le fonctionnement des systèmes de détection d'intrusion pour les centres de données principaux et secondaires du Siège (New York et New Jersey) et les pôles informatiques de la Base d'appui de Valence (Espagne) et de la Base de soutien logistique de Brindisi (Italie), ainsi que regroupement des sources de cyberveille du Secrétariat.

5. En réponse à sa question demandant où en étaient l'achat et l'installation des systèmes de filtrage des sites Web et des messages électroniques, le Comité consultatif a été informé qu'un dispositif de filtrage de pointe avait été acheté dans le cadre d'un contrat existant et était en cours d'installation, ce qui nécessitait des modifications de l'infrastructure sous-jacente et l'ajustement de la politique en vigueur en matière de filtrage des sites. L'achat du système avancé de filtrage des messages électroniques a fait l'objet d'un appel d'offres lancé en mars 2013 et encore en cours. En attendant l'adjudication du marché, un contrat de location-bail à court terme a été conclu à titre de mesure provisoire, avec prise d'effet à la fin novembre 2013. **Le Comité consultatif recommande que le Secrétaire général soit prié de fournir, dans son prochain rapport sur la question, les assurances que les produits et services acquis aux fins de l'application du plan d'action concernant la sécurité informatique ont été achetés au prix le plus juste**.

6. Au sujet de la formation sur ordinateur mentionnée au paragraphe 10 a) du rapport du Secrétaire général, le Comité consultatif a été informé qu'un contrat d'un montant de 35 826 euros avait été signé pour un cours de formation à la sécurité informatique couvrant le « tronc commun » identifié par le groupe d'intérêt pour la sécurité informatique à l'échelle du système des Nations Unies. Le cours sera obligatoire pour tous les membres du personnel et devrait démarrer au début de 2014 sur la plateforme commune d'apprentissage en ligne du Secrétariat (Inspira).

Le Comité engage le Secrétaire général à continuer de privilégier la collaboration à l'échelle du système et de rechercher toutes les possibilités de coopération supplémentaire et de mutualisation des solutions de sécurité informatique entre les organismes du système des Nations Unies.

7. Le Secrétaire général indique que, outre les mesures prises dans le cadre du plan d'action, l'Organisation introduit d'importants changements dans ses opérations informatiques à l'échelle mondiale, afin de mieux contrôler l'accès aux systèmes et de réduire la vulnérabilité aux intrusions afin de faciliter la mise en service du progiciel de gestion, Umoja. Peuvent être citées par exemple la mise en service d'un nouveau réseau longue distance mondial, l'utilisation d'un système d'accès standard (Citrix) pour tous les progiciels de gestion et la migration des applications vers les pôles informatiques de Valence et Brindisi. **Le Comité consultatif recommande que l'Assemblée générale prie le Secrétaire général d'accélérer dans la mesure du possible la migration des applications vers les pôles informatiques et de présenter un état détaillé des progrès accomplis dans le rapport susmentionné sur la nouvelle stratégie informatique**.

8. Le Secrétaire général indique aussi que le Bureau de l'informatique et des communications a décidé, en juillet 2013, de demander une évaluation indépendante de la sécurité informatique au Secrétariat, portant essentiellement sur l'infrastructure au Siège (A/68/552, par. 8). Il affirme que l'évaluation a validé et corroboré ce qui avait été détecté en interne et qu'elle a également révélé entre autres ce qui suit : a) les dispositifs de contrôle de la sécurité informatique en place à l'ONU sont insuffisants, tant pour les éléments classiques que pour les éléments qui n'avaient pas de commandes numériques auparavant tels que les systèmes d'administration des bâtiments, le contrôle et la surveillance des accès, les systèmes de téléphonie et de vidéoconférence et le matériel audiovisuel; b) le Département de l'appui aux missions a besoin de nouveaux logiciels pour assurer la surveillance et le filtrage nécessaires pour lutter contre les intrusions et mettre les pare-feux à niveau de manière à renforcer la sécurité tant au Siège que dans les autres sites; et c) il importe de surveiller de près les sites Web hébergés sur des serveurs extérieurs, passer en revue les dispositifs de sécurité et aider les départements du Secrétariat à revoir la conception de leurs sites afin de les protéger contre les intrusions ou les dégradations (ibid., par. 13 à 15).

9. Le Secrétaire général explique aussi que les systèmes informatiques du Secrétariat tendent à être de plus en plus interdépendants et à fonctionner en réseau et qu'une attaque ou une intrusion, où qu'elle se produise, risque donc de mettre en péril l'ensemble des sites, de sorte que les mesures prises pour exécuter le plan d'action au Siège devront être mises en œuvre dans les autres lieux d'affectation et s'accompagner d'un renforcement notable de la capacité de contrôle de l'Organisation (A/68/552, par. 18). De plus, du fait du caractère fragmenté du réseau informatique de l'Organisation, la sécurisation informatique est plus difficile et coûteuse. Le Secrétaire général indique que la stratégie de l'Organisation consiste à déménager promptement ses centres informatiques à Valence et Brindisi afin de pouvoir appliquer des mesures de sécurité et de contrôle plus rapidement et de réduire les coûts, et il précise que la défragmentation du réseau sera un élément central de la nouvelle stratégie informatique susmentionnée (ibid., par. 20).

10. **Le Comité consultatif prend note des progrès accomplis dans l'application du plan d'action au chapitre du règlement des problèmes de sécurité**

informatique et note que le Secrétariat a l'intention de réduire la fragmentation et les coûts dans le déploiement des mesures de sécurisation et de surveillance. Le Comité fait les mêmes observations que dans son rapport précédent au sujet de la sécurité informatique et reste préoccupé par le fait que la question ne soit traitée que très en aval (A/67/770 par. 68).

11. **De plus, compte tenu de l'envergure mondiale de l'ONU et du vaste champ de ses systèmes informatiques, le Comité consultatif estime qu'il importe de protéger l'Organisation contre la surveillance, l'interception et la collecte massives de ses communications et données, et recommande que l'Assemblée générale prie le Secrétaire général de proposer dans son prochain rapport des options possibles pour assurer une telle protection.**

Gouvernance, risque et respect des normes

12. Dans le domaine de la gouvernance, du risque et du respect des normes, le Secrétaire général fait état des mesures suivantes : a) publication d'une directive sur la sécurité informatique à l'usage de tous les chefs de départements et bureaux afin d'encadrer les orientations, les procédures et la marche à suivre en la matière dans l'Organisation; b) mise au point de 52 règles et procédures pour améliorer la performance et la sécurité des systèmes et l'intégrité de la production; c) création d'un groupe de travail pour la sécurité informatique relevant du Groupe de coordination de la gestion des questions informatiques afin que les bureaux extérieurs communiquent davantage entre eux; d) mise en place d'un mécanisme permettant de mieux veiller au respect des règles et procédures internes et des bonnes pratiques du secteur de l'informatique; et e) validation par le Réseau technologies de l'information et des communications du Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination, d'une série de critères minimum de sécurité informatique mis au point par le Groupe d'intérêt pour la sécurité informatique du Conseil en collaboration avec le Bureau de l'informatique et des communications. De plus, grâce au cadre général pour la sécurité informatique établi récemment par le Département de l'appui aux missions, des évaluations de la sécurité des systèmes, infrastructures et autres moyens informatiques déployés sont régulièrement effectuées à Brindisi et à Valence, ainsi que dans les missions [A/68/552, par. 10 d)].

13. Le Comité consultatif a demandé des précisions sur le cadre général pour la sécurité informatique mentionné au paragraphe 10 d) du rapport du Secrétaire général, notamment sur la question de savoir comment le Bureau de l'informatique et des communications collaborait avec le Département de l'appui aux missions pour les questions relatives à la sécurité informatique, quels étaient les mécanismes de coordination ainsi que le rôle qui leur était assigné et leurs responsabilités respectives. Il a été informé que le cadre en question s'appliquait à la fois au Département de l'appui aux missions du Siège et aux missions elles-mêmes. Le Département avait mis au point un cadre général de sécurité informatique spécialement conçu en fonction des besoins opérationnels et de l'environnement particulier des missions ainsi que des facteurs de risque présents sur le terrain. De plus, le Bureau de l'informatique et des communications agit en liaison et en coordination permanentes avec le Département afin de s'assurer que les directives particulières données aux missions sont dûment alignées sur les normes mondiales et les politiques et recommandations du Secrétariat. Par ailleurs, le Bureau et le Département ont tenu des consultations régulières et ont continué de collaborer

étroitement en ce qui concerne les systèmes communément utilisés et les informations/données partagées sur les atteintes à la sécurité informatique et les faiblesses des systèmes.

14. **Le Comité consultatif prend note de la publication d'une directive sur la sécurité informatique applicable à l'ensemble du Secrétariat. Il recommande que l'Assemblée générale prie le Secrétaire général de poursuivre ses efforts de manière à obtenir l'adoption de politiques et procédures communes en matière de sécurité informatique selon un schéma garantissant l'application du principe de responsabilité à tous les niveaux de l'Organisation. Le Comité reste d'avis que le Secrétaire général devrait prendre rapidement des mesures correctives pour lever les éventuels obstacles entravant la promulgation et la mise en œuvre des politiques communes de sécurité informatique au sein du Secrétariat.**

15. **De plus, étant donné que le Secrétaire général considère qu'une attaque ou une intrusion, où qu'elle se produise dans le réseau, risque de mettre en péril l'ensemble des sites, et qu'il faut donc appliquer des mesures de sécurité et surveiller les systèmes dans tous les lieux d'affectation, le Comité consultatif insiste sur la nécessité d'adopter une approche institutionnelle commune de la sécurité des systèmes informatiques du Secrétariat de manière à éviter les initiatives redondantes et les doubles dépenses dans ce domaine. Le Comité recommande que l'Assemblée générale prie le Secrétaire général de faire en sorte que la stratégie à moyen et à long terme pour la sécurité informatique présentée dans le cadre de la nouvelle stratégie informatique (voir plus haut, par. 3) soit fondée sur les règles et outils communs et qu'elle remédie à la fragmentation actuelle des systèmes de sécurité informatique de la manière la plus économique et la plus efficace possible.**

Questions diverses

16. Le Comité consultatif rappelle que l'Assemblée générale a approuvé l'utilisation de la base d'appui de Valence (Espagne) comme centre de communications secondaire actif et centre informatique (voir les résolutions 63/262 et 66/246). **Le Comité consultatif recommande de nouveau que l'Assemblée générale demande au Secrétaire général de veiller à ce que, dans tous les documents soumis à l'Assemblée générale, le centre de Valence soit désigné d'une manière cohérente qui reflète le rôle qu'il joue dans le domaine de l'informatique et des communications (voir A/67/780/Add.10, par. 29 à 31)**.

III. Ressources nécessaires

17. À sa demande, le Comité a reçu des informations sur les crédits approuvés par l'Assemblée générale au cours des cinq dernières années au titre de la sécurité informatique et les dépenses effectivement engagées à cette fin, ainsi que des renseignements détaillés sur les montants dépensés dans ce domaine au cours de l'exercice 2012-2013, qui figurent respectivement aux annexes II et III au présent rapport. Il note que les dépenses relatives à la sécurité informatique ont presque quadruplé, passant de 1,1 million de dollars en 2010-2011 à près de 4,1 millions de dollars en 2012-2013.

18. S'étant renseigné sur le montant des ressources qu'il était envisagé de consacrer à la gestion des risques de sécurité auxquels étaient exposés les logiciels

devant être remplacés par Umoja, le Comité consultatif a été informé que certains de ces logiciels étaient hébergés sur des systèmes d'exploitation très vulnérables, les fournisseurs n'en assurant plus l'appui technique ni les mises à jour de sécurité, et qu'il fallait donc si possible utiliser ces logiciels sur un autre système d'exploitation, ou, à défaut, les soumettre aux contrôles supplémentaires proposés afin de détecter toutes failles plus rapidement et d'en atténuer l'impact. **Tout en convenant de la nécessité d'assurer la sécurité des systèmes informatiques afin de protéger les installations de l'Organisation, le Comité consultatif insiste sur le fait qu'il convient de limiter au minimum le montant des ressources consacrées aux logiciels qui seront bientôt remplacés par Umoja**.

Ressources demandées pour 2014-2015

19. Pour l'exercice biennal à venir, le Secrétaire général propose notamment : a) de déployer le dispositif de détection d'intrusions et les systèmes de filtrage dans les bureaux hors Siège et les commissions régionales; b) de mettre le pare-feu à niveau; c) de renforcer les dispositifs de contrôle de sécurité internes; d) de mettre en place un système de gestion des risques permettant à l'Organisation de déceler les failles en amont et d'y remédier à titre prioritaire; e) de mener des activités de contrôle et de détection supplémentaires pour protéger les éléments d'infrastructure non classiques du Siège et l'environnement informatique des bureaux hors Siège, des commissions régionales et des centres informatiques de Valence et de Brindisi.

20. À cette fin, un montant supplémentaire de 3 440 700 dollars est demandé, réparti comme suit : a) 581 400 dollars au titre des autres dépenses de personnel, pour couvrir les services de personnel temporaire (autre que pour les réunions), à savoir un informaticien spécialiste de la sécurité (P-4), chargé d'aider à mettre en œuvre le nouveau système de détection d'intrusions, et deux informaticiens (P-3) chargés d'exécuter les nouvelles fonctions d'analyse des logiciels malveillants, de développement de patrons de conception et de corrélation et de renforcer les capacités existantes en matière de contrôle des intrusions, d'évaluation de la vulnérabilité des systèmes, de génération de rapports et de coordination des contrôles de sécurité des applications Web; b) 150 000 dollars au titre des voyages, pour financer les voyages de deux membres du personnel dans tous les bureaux hors site, les commissions régionales et les centres informatiques de Valence et Brindisi pendant au moins deux semaines; c) 1 325 000 dollars au titre des services contractuels, qui couvriront le déploiement et le fonctionnement continu des systèmes de détection des intrusions (800 000 dollars) et d'un système de gestion des vulnérabilités (25 000 dollars) ainsi que les services d'experts chargés d'exécuter les activités nécessaires à la mise en œuvre de la stratégie de sécurité informatique du Secrétariat (500 000 dollars); 1 325 000 dollars au titre du mobilier et du matériel, qui permettront de financer la mise à niveau du pare-feu (1 000 000 dollars), la surveillance du réseau en continu (200 000 dollars) et le contrôle de la sécurité des applications Web (125 000 dollars); e) 59 300 dollars au titre des frais généraux de fonctionnement.

21. Ayant demandé des précisions, le Comité consultatif a été informé que le montant demandé au titre du chapitre 29E du projet de budget-programme pour 2014-2015 comprenait des crédits destinés à financer la poursuite de certaines tâches relatives à la gestion des risques et à la sécurité informatiques, comme suit : a) l'élaboration et l'actualisation de la politique de sécurité informatique et le contrôle de son respect dans l'ensemble de l'Organisation; b) l'appui aux activités

d'évaluation et d'atténuation des risques; c) la coordination et la fourniture d'une assistance en matière de gestion des incidents de sécurité; d) la coordination des réponses aux recommandations d'audit et de la suite qui leur est donnée; e) le traitement de toutes les demandes d'accès à IMIS (y compris à distance) et au Sédoc, des demandes d'accès à distance au système Nucleus et des autres questions liées à la sécurité de l'accès aux systèmes. En ce qui concerne les effectifs existants, le Comité a été informé que le Groupe de la sécurité informatique et de la gestion des risques de la Section de la sécurité et de l'architecture informatiques du Bureau de l'informatique et des communications comprenait un spécialiste de la sécurité informatique (P-4), un spécialiste de la sécurité informatique (P-3) et deux assistants à la sécurité informatique [agent des services généraux (Autres classes)], ainsi qu'un responsable du contrôle de conformité et un spécialiste de la reprise après sinistre, recrutés sur des emplois de temporaire à la classe P-4. En outre, dans la plupart des autres départements et bureaux, les activités relatives à la sécurité informatique étaient confiées à des membres du personnel et des sous-traitants qui effectuaient également d'autres tâches. D'après une étude menée au début de 2013, l'équivalent de 12,5 postes à plein temps d'administrateur et d'agent des services généraux étaient consacrés à la sécurité informatique dans l'ensemble du Secrétariat.

22. Le Comité consultatif rappelle que, dans sa résolution 67/254, l'Assemblée générale a prié le Secrétaire général de lui rendre compte, dans le projet de budget-programme pour l'exercice 2014-2015, des questions liées à la sécurité informatique. **Bien que le Secrétaire général ait déclaré que ses propositions étaient en partie basées sur les conclusions de l'analyse des conditions de sécurité effectuée en juin 2013, y compris la proposition visant à élargir la portée des activités menées en 2014 afin de renforcer encore la sécurité informatique dans les bureaux hors Siège, les commissions régionales et les missions, le Comité consultatif estime que certaines des ressources supplémentaires demandées dans son rapport auraient déjà pu être prévues dans le projet de budget-programme pour 2014-2015. De surcroît, le Comité note que les propositions du Secrétaire général portent sur des dépenses à caractère structurel et renouvelables qui nécessiteraient la révision du programme de travail du Bureau de l'informatique et des communications approuvé pour la période 2014-2015 (voir A/67/6/Rev.1, programme 25). Le Comité recommande que l'Assemblée générale demande au Secrétaire général de faire tout son possible pour que les prévisions de dépenses relatives à des besoins renouvelables figurent dans le budget-programme biennal afin de faciliter son examen des ressources demandées pour le Bureau de l'informatique et des communications**.

23. **En outre, compte tenu de la nécessité d'adopter une stratégie de sécurité informatique commune à l'ensemble du Secrétariat et reposant sur des politiques et des outils communs (voir par. 14 et 15 plus haut), le Comité consultatif recommande que l'Assemblée générale demande au Secrétaire général de répartir les dépenses relatives à la sécurité informatique sur la base de la même formule de partage des coûts que celle utilisée pour le financement du progiciel de gestion intégré (voir la résolution 63/362 de l'Assemblée).**

IV. Conclusions et recommandations

24. La décision que l'Assemblée générale est appelée à prendre est énoncée au paragraphe 30 du rapport du Secrétaire général. Le Comité consultatif recommande que l'Assemblée générale prenne note du rapport du Secrétaire général en tenant compte des observations et recommandations formulées dans le présent rapport. **Le Comité recommande également que l'Assemblée générale prie le Secrétaire général : a) d'imputer toutes dépenses supplémentaires au titre des emplois de temporaire et des voyages sur les crédits alloués à ces rubriques dans le projet de budget-programme pour l'exercice 2014-2015; b) de rendre compte, dans le rapport sur l'exécution du budget pertinent, de toutes dépenses supplémentaires engagées au titre des services contractuels (A/68/552, par. 27) ou du mobilier et du matériel (ibid., par. 29).**

Annexe I

Récapitulatif des problèmes de sécurité détectés et de leurs solutions

Problème	*Solution*	*Descriptif*
Incapacité de surveiller ou de détecter le trafic réseau résultant d'activités dissimulées ou avancées menées de façon continue par des groupes liés à des attaques avancées persistantes. Manque de visibilité du réseau.	Services de détection des intrusions	Les services de détection des intrusions se chargeront de disposer les équipements de façon stratégique dans le réseau pour assurer la visibilité de l'ensemble du trafic. Cela permettra de lancer des alertes en cas d'activités suspectes et de saisir le trafic réseau en temps réel. Ces alertes seront transmises à une société d'appui qui dispose d'une équipe de spécialistes chargés de les examiner et d'adresser aux services chargés de la sécurité informatique de l'ONU des notifications urgentes exploitables.
Mise en danger continuelle d'équipements de l'ONU tels que les postes de travail ou les ordinateurs de bureau par suite de l'utilisation de logiciels malveillants, hautement personnalisés, envoyés par courriel; le nombre d'attaques de ce type enregistrées au cours des neuf premiers mois de 2013 est supérieur de 76 % au nombre total d'attaques constatées en 2012	Filtrage avancé du courrier électronique	Les logiciels malveillants personnalisés sont conçus pour se soustraire à la détection pouvant être réalisée grâce aux solutions antivirus classiques. La solution du filtrage avancé utilise des techniques qui analysent le comportement de ces fichiers pour détecter des codes malveillants qui, selon toute vraisemblance, ne le seraient pas par les solutions existantes.
Incapacité de se protéger contre les attaques avancées persistantes	Pare-feu de la nouvelle génération	Nombre d'attaques sont désormais conçues pour contourner les pare-feu classiques. Les applications de la nouvelle génération ou les dispositifs modernes de protection par pare-feu, qui effectuent des opérations supplémentaires pour mettre l'organisation à l'abri, ont été mises en place à New York et dans deux pôles informatiques. Les ressources demandées ont pour objet d'étendre cette capacité à l'ensemble des installations en vue d'assurer une protection uniforme du réseau de l'Organisation. Les ressources en personnel demandées sont indispensables pour assurer la configuration initiale et le fonctionnement du système
Incapacité de corréler les données issues de systèmes multiples afin de déterminer des tendances de l'activité et de référencer les données rétrospectives (enregistrées) du système. Manque de visibilité	Suivi permanent (analyse des journaux d'exploitation)	Ce dispositif recueille les journaux d'exploitation provenant d'un grand nombre de systèmes afin de déterminer les tendances des attaques dans l'ensemble du réseau et offre les moyens d'établir rapidement la chronologie d'une attaque lorsque celle-ci est détectée. Il est

Problème	*Solution*	*Descriptif*
		indispensable pour l'utilisation globale de tout les systèmes de sécurité. Les ressources en personnel demandées sont essentielles pour la configuration initiale et le fonctionnement du système
Insuffisance des ressources disponibles aux fins de déterminer précisément les sources des attaques et l'étendue des dommages résultant d'une intrusion	Analyse des codes malveillants, recherche de preuves informatiques et intervention en cas d'intrusion	Les ressources en personnel demandées apporteront la capacité de déterminer rapidement si des informations ont été perdues par suite d'une intrusion, ou comment s'est déroulée l'attaque, ce qui complétera et augmentera l'ensemble des compétences du personnel de l'Organisation dans ce domaine.
Non-respect des procédures établies et non-exécution des mises à jour et des correctifs des systèmes de l'Organisation, se traduisant globalement par une plus grande vulnérabilité	Évaluations de la vulnérabilité	Utilisation d'un logiciel assurant automatiquement le suivi permanent et la vérification du respect des procédures établies pour faire en sorte que tous les systèmes de l'Organisation soient à jour et pour déterminer les vulnérabilités subsistantes.

Annexe II

Estimation des dépenses au titre des technologies de l'information et des communications (TIC) depuis 2010, par année et par exercice biennal

(En dollars des États-Unis)

	Exercice biennal 2010-2011			*Exercice biennal 2011-2013*		
	2010	*2011*	*Total*	*2012*	*2013*	*Total*
Postes	318 000,00	318 000,00	636 000,00	719 600,00	773 450,00	1 493 050,00
Consultants		177 221,00	177 221,00	112 777,00		112 777,00
Formation				436,67		436,67
Frais de voyages des consultants spécialistes de la norme ISO 27001				14 130,00	2 995,00	17 125,00
Évaluations de la sécurité indépendantes					60 000,00	60 000,00
Évaluations de la conformité à la norme ISO 27001	24 000,00	33 025,49	57 025,49	38 170,90	1 545,00	39 715,90
Logiciel spécialisé de protection des serveurs		64 276,10	64 276,10	7 122,15	7 122,15	14 244,30
Logiciel de protection des postes de travail	4 144,50	193 435,18	197 579,68	234 711,39	300 611,97	535 323,36
Logiciel de gestion et de contrôle du respect des procédures établies				19 703,00		19 703,00
Filtrage avancé du courriel au Siège de l'ONU					200 000,00	200 000,00
Pare-feu pour le Siège de l'ONU				307 968,80	540 000,00	847 968,80
Mesures supplémentaires du plan d'action pour les TIC					715 158,00	715 158,00
Total	**346 144,50**	**785 957,77**	**1 132 102,27**	**1 454 619,91**	**2 600 882,12**	**4 055 502,03**

Annexe III

Dépenses engagées au cours de l'exercice biennal 2012-2013 au titre de la sécurité informatique

(En dollars des États-Unis)

Intitulé	*Descriptif*	*Prix*	*Quantité*	*Total*
1. Achats effectués sur bon de commande (valeur unitaire inférieure à 4 000 dollars)				
Logiciel pour tester la sécurité des sites Web	Plateforme intégrée permettant de tester la sécurité des applications Web. Application unique comportant un grand nombre d'éléments personnalisés et professionnels pouvant être utilisés par des vérificateurs chevronnés. Faible coût, grande utilité	300	2	600
Logiciel élémentaire de détection des vulnérabilités	Instrument automatisé d'analyse des vulnérabilités réseau/serveur – faible coût, permet l'utilisation de plusieurs serveurs	3 900	1	3 900
Outils de renseignement et d'analyse	Application à source ouverte de renseignement et de recherche de preuves informatiques, avec application d'analyse des dossiers	760 + 200	1	960
Logiciel de recherche de preuves informatiques	Ensemble performant d'outils de recherche de preuves informatiques pouvant être utilisés sur les ordinateurs de bureau, les serveurs et les appareils mobiles	2 999 + 599	1	3 598
Outil permettant la connexion de disques durs à des fins de diagnostic	Outil utilisé pour connecter en externe à un ordinateur un disque dur SATA pour des travaux de copie ou de diagnostic	75	2	150
Total partiel				**9 208**
2. Achats faisant l'objet d'une demande de devis (valeur unitaire inférieure à 40 000 dollars)				
Outil d'examen de la sécurité des sites Web	Logiciel de test et d'analyse de la sécurité des sites Web	5 950	1	5 950
Outil d'analyse de la sécurité des sites Web	Logiciel de test et d'analyse de la sécurité des sites Web	20 300	1	15 000
Logiciel de gestion des pare-feu	Logiciel de gestion et de suivi des règles de pare-feu	35 000	1	35 000
Total partiel				**55 950**
3. Achats faisant l'objet d'un appel d'offres (valeur unitaire comprise entre 30 000 et 200 000 dollars)				
Services contractuels (expert pare-feu)	Recours aux services d'un consultant externe à l'appui de la refonte du réseau et de la mise en place des pare-feu, pour une durée d'un mois, fin novembre ou début décembre	40 000	1	40 000
Total partiel				**40 000**

Intitulé	*Descriptif*	*Prix*	*Quantité*	*Total*
4. Achats faisant l'objet d'une demande de proposition				
Cours de sensibilisation à la sécurité informatique	Mise au point d'un module de sensibilisation à la sécurité informatique au format HTML5, à intégrer dans Inspira	30 000	1	30 000
Système avancé de filtrage du courriel	Acquisition des dispositifs et logiciels fire eye e-mail MPS, assortie d'un recours à des services professionnels de filtrage avancé du courrier électronique	230 000	1	230 000
Pare-feu Checkpoint offrant une protection au niveau 7	Achat de plusieurs pare-feu Checkpoint offrant une protection au niveau 7, complétés par checkpoint firewall software blade	540 000	1	540 000
Services de sécurité gérés	Passation d'un marché pluriannuel de services de sécurité gérés, comprenant le matériel, le logiciel et le recours à des compétences extérieures pour la surveillance du réseau	350 000	1	350 000
Total partiel				**1 150 000**
Total				**1 255 158**