联合国 A/68/552

大 会

Distr.: General
25 October 2013
Chinese
Original: English

第六十八届会议

议程项目 134

2014-2015 两年期拟议方案预算

关于加强全秘书处信息和系统安全的建议执行进展情况

秘书长的报告

摘要

本报告是按照大会第 67/254 号决议第一部分第 18 段提交的。该段请秘书长在 2014-2015 两年期拟议方案预算中介绍处理信息安全问题各项行动的最新执行情况。一项独立评估以及 2013 年发生的信息安全受损事件表明，这方面存在重大缺陷，使本组织面临严重到无法接受的风险。本报告论述了为防止网络攻击威胁而采取的各项措施，也提出 2014-2015 年两年期拟议方案预算第 29 E款(信息和通信技术厅)项下需追加重计费用前资源 3 440 700 美元，以解决本组织最紧迫的信息安全需要。

13-53215 (C) 051113 061113

一. 导言

1. 大会第 66/246 号决议第 107 段要求行政和预算问题咨询委员会请审计委员会审计和评价秘书处包括信息和通信技术厅处理信息和通信技术(信通技术)事务的工作，并在大会第六十七届会议主要会期报告有关情况。审计委员会于 2012 年 10 月进行了审计，并于 2012 年 12 月 19 日向秘书长提交了报告(A/67/651)。

2. 审计委员会在报告第 95 段中指出，联合国不具备足够安全的信息环境，且现有的安全控制措施未达到审计委员会对现代全球组织的期望水平。审计委员会又说，秘书处进行安全监测的能力极为有限，因此无法充分发现和应对所有企图损害安全或已经损害安全的情况。

3. 秘书长在随后的一份报告论述了审计委员会建议的执行情况(A/67/651/add.1)。他说，目前正在紧急处理关于加强全秘书处信息和系统安全的建议，且行政当局正在拟定行动计划，其中包括采取短期措施以处理最紧急的缺陷，并确定信息安全问题的可持续中长期战略。行动计划包括 3 个领域的 10 项举措，即：

(a) 预防性控制。秘书处将加强对信通技术基础设施的技术控制，以便：

㈠ 对联合国网络上使用的计算装置实施更严格的控制；

㈡ 通过加强技术措施，保护联合国网络边界，防止有害形式的互联网内容和电子邮件；

㈢ 将网络各部分隔开，以孤立可能隐藏有潜在攻击性病毒的区域；

㈣ 开展培训和宣传，提高联合国工作人员的信息安全意识；

(b) 提高事件侦测和回应能力。为适应各种威胁风险大幅提高的环境，秘书处将采用补充入侵探测系统，并对其网络进行系统监测；

(c) 治理、风险和合规。将批准和执行一项信息安全指示，其中规定联合国信息安全基本原则，作为政策和治理工具的基础。

4. 行政和预算问题咨询委员会评论了审计委员会关于秘书处信息和通信技术事务处理情况的报告(A/67/770)，最后建议请秘书长在制定信息安全行动计划执行提议时，尽一切努力确定重点并调拨资源，同时尽可能避免提出追加资源的要求。行预咨委会还说，它和审计委员会同样对信息安全状况表示关切。行预咨委会建议，应请秘书长将执行其行动计划作为优先事项推进，并确保不再拖延地通过信息安全章程和相关政策文件，以确保在联合国所有各级落实问责制。此外，行预咨委会还提出，秘书长应及时采取补救行动，解决可能妨碍在整个秘书处内有效实施行动计划或颁布和执行信息安全政策的任何障碍。行预咨委会建议请秘书长在 2014-2015 两年期拟议方案预算中说明关于解决信息安全问题的行动的最新执行情况。行预咨委会还请审计委员会就其对此提出的建议的执行情况采取后续行动。

5. 此后，大会第 67/254 号决议第一部分第 11 段请秘书长提出一项进度报告，说明采取了哪些措施处理审计委员会报告(A/67/651)确认的优先事项，包括提供关于信息安全的资料。大会还在第 18 段中请秘书长在 2014-2015 两年期拟议方案预算中介绍处理信息安全问题各项行动的最新执行情况，包括防止网络攻击威胁的各项措施的最新执行情况。

二. 现状

6. 秘书长正在积极推进加强整个秘书处信息安全的行动计划，并已集中精力应对总部最紧急、最关键的行动领域。迄今为止，信息和通信技术厅已尽一切努力在核定批款范围内调整资源使用重点和调拨资源，以尽可能吸收行动计划各项倡议执行活动的费用。但事实证明这些资源并不足以充分应对已查明的所有缺陷。另外，自审计委员会报告发布以来，全球信息安全受损情况已显著增加，次数更多，复杂性更高，其中一些是秘书处直接遭受的损害。

7. 由于发生了这些事件，秘书长认为必须采取紧急行动，范围应超出信息和通信技术厅迄今所采取的行动。

三. 加强信息安全行动计划的初步执行步骤

8. 行动计划旨在紧急应对最紧迫的信息安全缺陷，并为秘书处制定可持续的中长期信息安全战略。鉴于缺乏内部专门知识，而且需要对本组织的安全态势作出详尽分析，确定需要外部专门知识，以便核查和(或)核实潜在风险。2013 年 7 月，信息和通信厅聘请外部咨询公司对秘书处信息安全状况进行独立评估，证实和补充了内部审查结果，并确定了本组织信息安全领域的弱点和业务缺陷。该独立评估以及 2013 年全年发生的更多信息安全事件表明，这方面存在重大缺陷，使本组织面临无法接受的危险。

9. 独立评估的重点是纽约的基础设施。秘书长根据评估认为，鉴于对本组织的网络攻击次数有所增加，2014 年必须进一步加强总部的信息安全，紧急扩大独立评估范围，同时扩大有关活动的范围，以进一步加强总部以外办事处、区域委员会、外地特派团的信息安全。与这些办事处合作获得的信息表明，需要开展大量工作才能应对这些办事处存在的弱点。同样，虽然由外勤支助部提供支助的外地办事处弱点较少，但鉴于这种服务由西班牙巴伦西亚联合国支助基地和意大利布林迪西联合国后勤基地集中提供，因此仍须彻底评估其弱点。

10. 以下详述迄今已开展的落实行动计划活动：

(a) 加强了预防性控制，包括针对新发给和(或)更新的台式计算机和膝上型计算机限制行政特权。现正在购置更多电子邮件和互联网内容过滤系统，预计将于 2013 年 11 月底前完成。此外，还在按当前安全补丁要求重新配置服务器，以

确保服务器在消除潜在弱点方面达到最新要求。已审查了总部防火墙基础设施，正以更先进技术取代之，以加强对外来攻击的防护，并进一步隔开内部网的各部分。另外，还购置了一个基于计算机的培训课程，用以提高秘书处所有工作人员对信息安全的意识；

(b) 已开始评估目前在运行的所有软件应用程序，以确保其符合信息安全标准和最佳做法。这项活动的范围包括，查明执行“团结”项目和其他企业系统后将继续运行的所有应用软程件序，并确保它们不构成安全风险；

(c) 已为纽约和新泽西主用数据中心和备用数据中心的主数据中心以及支助基地和后勤基地的企业数据中心购置管理服务，以部署和持续运行入侵探测系统。此外，还合并了整个秘书处现有的网络情报来源，使秘书处能主动调整防御措施；

(d) 制定了一项信息安全政策指示，于 2013 年 3 月 7 日发给各部厅首长，作为本组织信息安全政策、程序和准则的总框架。该指示还规定须报告信息安全事件，并须分享整个秘书处的有关行动情报。联合国系统行政首长协调理事会(首协会)的信息安全特别兴趣小组根据信息和通信技术厅的草案制定了一套公共网站技术和程序管制最低要求。这些要求已获得首协会管理问题高级别委员会内信息技术网络的核可。此外，正在制定 52 项信通技术政策和程序，以利增强系统性能、安全、工作成果完好性。2013 年将与新闻部合作，把该文件作为行政指示发布，以应对公共网站的大规模风险，并解决以往几次有证据的安全受损情况。此外，信息和通信技术厅还重新分配资源，以建立内部合规职能部门，负责增强对内部政策和程序以及业内最佳做法的遵守。该厅还设立了信息安全工作组，作为信通技术管理协调组的一部分，负责增强总部以外办事处、区域委员会、外地特派团等工作地点之间的沟通。

11. 除根据行动计划采取措施外，本组织还在对全球信通技术业务启动重大改革，以遵守和配合落实“团结”项目以及其他辅助系统。这些改革主要包括：采用基于多协议标志交换的新全球广域网；全部企业系统采用标准接入层(思杰)；向巴伦西亚和布林迪西企业数据中心转移软件应用程序。这些变革有助于加强出入管制，有利于更稳健地管理信通技术基础设施，并可使其不易受到侵害。

12. 信通技术安全是业务连续性和灾后恢复的重要组成部分。鉴于外地特派团的行动环境，信通技术安全对它们具有重要作用。外勤支助部最近建立了安保政策框架，主要针对该部的外地技术业务中心，包括支助基地和后勤基地的信通技术设施。根据该政策框架，目前定期在外地技术业务中心和外地特派团对已部署信息系统、基础设施和其他信息资产进行安全评估。

四. 需要的进一步行动

13. 独立评估和 2013 年出现信息安全受到破坏的情况显示，联合国没有设定足够的信息安全控制措施，不仅信息和通信基础设施的传统构成部分如此，而且其

他基础设施要件也是这样。传统上没有数字化控制的建筑物管理系统、出入控制和监测解决方案、电话技术及视频会议系统和视听设备，现在也暴露于数字化的和可能基于互联网的威胁之中。将需要更多的详细评估，以确保这些设备都被纳入一个全面信息安全战略。

14. 对外勤支助部所用系统的一次评估显示，需要新的软件工具取得入侵监测和过滤能力，同时将防火墙升级，以增强本组织上述两个地点和其他地点的安全环境。新的安全措施已经实施，更多的工作已在进行之中。

15. 还发现本组织的声誉风险有可能由于网络信息管理的业务缺陷而增高。因此，本组织已确定需要密切审视外部托管的网站，同时审查安全控制措施并为秘书处各部门重新设计网站提供协助，以防范入侵或污损。

16. 包括网基和非传统系统并解决根本性系统问题的全面信息安全战略将是信通技术整体战略的一个核心部分，将提交大会第六十九届会议审议。

17. 不过，就当下而言，急需在迄今通过实施加强整个秘书处信息安全行动计划所取得进展的基础上再接再厉，立即采取进一步行动继续缓解本组织面对的不可接受的风险。

18. 由于对相互连通性的需求不断增加和秘书处信通技术系统的相互依存，任何地方的一次攻击或入侵都可导致所有地方受损。因此，迄今为执行该行动计划而采取的措施也需要在其他工作地点实施，并辅以本组织监测能力的大幅度增强。

19. 在修订后信通技术战略提出之前，本报告建议以下列行动为临时措施，并请求为其提供资源：[1]

(a) 扩大入侵检测服务，以覆盖总部以外各办事处和各区域委员会。现已通过重新调整信息和通信技术厅 2013 年现有资源分配的优先次序设立这项服务，仅限于纽约和新泽西的主用和备用数据中心以及支助基地和后勤基地的企业数据中心。但是，2014 年将需要更多资源以涵盖已设立地点的服务费用和把覆盖范围扩大到海外工作地点；

(b) 增加防火墙基础设施的覆盖范围和将其升级，并将电子邮件和互联网讯息的过滤解决方案升级到覆盖总部以外各办事处和各区域委员会，以在全球加强网络安全能力；

(c) 加强内部安全监测能力。需要增加工具和工作人员资源以大幅度增强能力，监测信息和通信技术环境，查明未遂和得手的破坏信息安全行为；

[1] 由于这些行动的敏感性质和为了尽量减少业务风险，本报告中只可提供一般性说明。

(d) 部署一个脆弱性管理系统，以使本组织能够积极主动地查出具体弱点并优先对其进行弥补；

(e) 对总部的非传统基础设施要素和总部以外各办事处及各区域委员会的信息和通信技术环境以及位于巴伦西亚和布林迪西的企业数据中心进行保护和探测控制措施方面的更多评估。

20. 本组织信通技术网络各自为政的情况显然使确保安全变得更加困难和昂贵。本组织战略是从速将其数据中心迁往巴伦西亚和布林迪西，以能更快地部署安全和监测措施，同时改进业务绩效和减少费用。此外，消除各自为政的状态将是秘书长新信通技术战略的一个支柱，将提交大会第六十九届会议审议。

五. 2014－2015 年期间工作方案所需修改

21. 为妥善解决整个秘书处的信息安全问题，需要修订信息和通信技术厅核定的 2014-2015 年期间工作方案(A/67/6/Rev.1，方案 25)，以增加与执行次级方案 5(信息和通信技术的战略管理和协调)有关的活动。

六. 2014-2015 两年期拟议方案预算需要追加的资源

22. 本报告所列追加所需资源的出现，是秘书长提交了 2014-2015 两年期拟议方案预算(A/68/6(Sect.29E))后在 2013 年所进行一次独立评估的结果，而其依据则是联合国所受网络攻击的数量和频率的增加。因此，将需要增加批款以涵盖上文详述活动的实施。

23. 如下文表 1 所详示，第 29E 款下 12 个月期间估计在重计费用前总共需要 3 440 700 美元，解决本报告中详述的本组织最紧迫的信息安全需要，以待大会第六十九届会议对修订后信通技术战略进行审议。

表 1

按支出用途开列的所需经费总表

(千美元)

支出用途	2014-2015 年估计数
其他工作人员费用	581.4
工作人员差旅费	150.0
订约承办事务	1 325.0
般业务费用	59.3
家具和设备	1 325.0
共计	**3 440.7**

表 2

2014-2015 两年期拟议方案预算第 29E 款下重计费用前所需资源

(千美元)

支出用途	A/68/6(Sect.29E)中提供的经费	追加所需资源	所需资源共计
员额	36 168.6	—	36 168.6
其他工作人员费用	5 634.0	581.4	6 215.4
工作人员差旅费	467.8	150.0	617.8
订约承办事务	12 697.0	1 325.0	14 022.0
一般业务费用	16 574.5	59.3	16 633.8
用品和材料	202.4	—	202.4
家具和设备	948.2	1 325.0	2 273.2
共计	**72 692.5**	**3 440.7**	**76 133.2**

其他工作人员费用

24. 581 400 美元的经费将涵盖 12 个月期间的一般临时人员，以履行职能，处理与信息和通信技术厅安全做法重新设计和应用及相关事件应对有关的紧迫安全关切。所需临时职位如下：

(a) 一个相当于 P-4 员额的一般临时职位，履行安保工程师的职责。这一职位将提供与应用最近实施的入侵探测系统有关的更多技术专长。估计本组织每月至少会发生 70 000 至 100 000 次安全警报。安保工程师将与一个外部订约人一道开展工作，有系统地确定和处理被认为需要立即行动的紧要警报。由于入侵探测系统将推出到总部以外各办事处和各区域委员会，它将收集全球范围的信息。各地点之间警报相关性和有关的事件应对活动必须得到全球协调。这一全球协调职能对于入侵探测系统提供的对网络更深入了解能力发挥功效至关重要。此外，安保工程师还可协助设立更高级防火墙分析和管理；

(b) 两个相当于 P-3 员额的一般临时人员职位，履行恶意软件分析、模式创建和事件相关性方面的新职能。这些职能对于确定本组织可能面临的全球各种行为体的所谓严重持续威胁的攻击类型具有关键意义。这些职位还将在渗透测试、脆弱性评估、报告生成和网络应用安全测试协调方面扩大现有能力。此外，这些职位还可能与软件开发团队互动，以加强全球各部门的安全开发标准和测试。

工作人员差旅费

25. 需要经费 150 000 美元，以涵盖两名工作人员前往总部以外所有办事处、区域委员会和位于巴伦西亚及布林迪西的企业数据中心为期至少两周的费用，以便：

(a) 立即进行独立的安全合规评估和技术测试，必须完成这些工作才能确保现行政策和标准作业程序日常得到遵守和执行。这次特派任务包括评估、验证和记录先前未记录的当地问题和信息安全风险。此外，此举还将使总部工作人员能够监测和报告合规水平，因此对于中央信通技术安全战略的实施至关重要；

(b) 为落实政策以及验证计划中的所有新系统和应用程序提供技术咨询和协助；

(c) 与所有业务及技术利益攸关方举行会议和进行现场实训，以确保预防性信息安全措施的设计和架构在所有工作地点都得到理解和有效落实。

26. 这一类别下的拟议资源将涵盖前往一些地点的差旅费，因为鉴于所涉工作的保密性质，在这些地点使用互联网和(或)声频会议技术并非有效的替代办法。将尽可能继续实行一次出差执行多项任务，以更有效地使用资源。

订约承办事务

27. 1 325 000 美元的经费将涵盖以下所需资源：

(a) 入侵探测事务(800 000 美元)，用于部署和持续运行入侵防范系统，这些系统已作为执行行动计划的一部分启动。已通过重新分配现有资源在纽约、布林迪西和巴伦西亚完成初期部署。不过，为实现全球全面覆盖，这一服务需要扩大到所有数据中心和工作地点。探测未遂入侵的能力对于本组织及时采取对策至关重要；

(b) 一个脆弱性管理系统(25 000 美元)，用于系统和定期地扫描联合国所有信通技术资产，包括服务器和其他关键系统，以确保其正确配置和及时部署关键安全更新措施，同时协助管理这类资产并在外部利用一些弱点实施攻击之前将弱点查出；

(c) 个人服务(500 000 美元)，用于获取高度专门化的知识专长，以视需要开展对于持续执行秘书处信息安全战略至关重要的活动，包括新建立的技术和对关键基础设施要素进行更多的评估。此外，还需要获得某些关键的知识专长，以处理短期的具体技术问题和提供更多的查证或调查能力，确保深入理解处理信息安全缺陷的方式。这一工作将属短期和高度专业性质，目的是把获得的知识传递给工作人员。

一般业务费用

28. 59 300 美元的经费将涵盖以下费用：为纽约三个临时职位租用办公空间(47 700 美元)和执行一项服务级别协议(“A”)(6 300 美元)；一个局域网(1 800 美元)；通信费(3 500 美元)。

家具和设备

29. 1 325 000 美元的经费将涵盖以下所需资源：

(a) 连续监测能力(200 000 美元)。对系统记录进行中央收集和分析，以补充入侵探测系统提供的资料，并使本组织能够探测到不被认为是恶意的异常或可疑活动。这样一种系统除有能力探测滥用和暗中破坏外，还将能在发现入侵后分析其根本原因和确定其范围。拟采购的安全信息和事件管理系统包含专门的硬件、软件和根据所收集信息的数量确定的许可证；

(b) 增强防火墙基础设施(1 000 000 美元)，包括以称为“下一代”的最先进防火墙和内容感知过滤器升级现有的防火墙(500 000 美元)和过滤解决方案(500 000 美元)，这将使本组织能够防止或探测专门躲避传统工具探测的未遂攻击和入侵。这次升级对于应对本组织所受性质不断变化的攻击至关重要。2013 年，已通过重新分配现有资源，在总部和位于巴伦西亚及布林迪西的企业数据中心启动升级。不过，增强措施必须扩大到所有的数据中心和工作地点；

(c) 网络应用安全测试(125 000 美元)，其中包括购置更新的网络应用安全测试工具，即以软件许可证形式购置在本地使用，或以第三方“软件作为服务”形式购置在全机构范围实施。这些工具可由内部安全人员和(或)网络开发人员用于加强联合国网站的安全。

七. 有待大会采取的行动

30. **请大会：**

(a) **注意本报告；**

(b) **为采取迫切需要的措施以加强秘书处信通技术安全，在 2014-2015 两年期拟议方案预算第 29E 款(信息和通信技术厅)下核准追加批款 3 440 700 美元，从应急基金中拨付。**