国 际 电 信 联 盟

ITU-T X.1126

(03/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务 – 移动安全

减缓移动网络中受感染终端负面影响的导则

ITU-T X.1126 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	**X.1120–X.1139**
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1379
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1126 建议书

减缓移动网络中受感染终端负面影响的导则

摘要

ITU-T X.1126建议书为移动运营商提供了采用技术手段遏制受感染终端，以保护用户和移动运营商的导则。该建议书描述了移动环境中不健康生态系统所导致的恶意软件的特性和影响。基于网络侧的技术，本建议书侧重于减缓受感染终端所引发的恶劣影响。本建议书定义并组织了缓解措施及对应的技术。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1126	2017-03-30	17	11.1002/1000/13194

关键词

感染、恶意软件、移动网络、终端。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

移动设备操作系统的迅速扩展和发展为移动行业带来了巨大的、充满活力的市场。围绕着这个价值不菲的市场，许多生态系统应运而生，以利用其带来的种种好处。但是，当前移动设备的强大能力也可被恶意软件滥用，被用来攻击终端、网络和业务的薄弱环节，由此造成重大损失。

注意到应在传统的移动系统中推行健康的生态系统，而不是使之成为一个“与世隔绝的花园”，从而确保移动市场的安全并保护所有相关合作伙伴的利益。在一些国家，健康的生态系统已取得了成功。

也应注意到，移动市场生态系统在某些国家高度多样化，尽管其中一些是不负责任、不健康甚至危险的。除恶意软件外，不负责任的生态系统带来的不利影响可对移动用户和网络带来重大损失。有时，甚至健康生态系统中的移动用户和网络可受到已感染终端的影响，因为当前绝大多数移动互联网业务是全球性的。

以下列举了主要在不负责任的生态系统中扩散的恶意软件的潜在风险：

对于用户而言：

- 隐私被窃，如窃听和位置跟踪；
- 财产损失，如系统异常和数据损毁；
- 恶意交易和消费，如发送昂贵的信息、拨打国际呼叫中心；
- 恶意软件传播，攻击其他终端；
- 发送垃圾邮件，骚扰其他用户；
- 欺诈和勒索。

对于运营商而言，对网络实体、移动业务和其他终端的攻击包括：

- 占用大量网络或移动业务的资源，危及服务并导致用户投诉服务质量；
- 劫持业务主机甚至网络实体。

出于以下原因，相比传统的有线互联网，恶意软件对移动互联网带来的危害更大：

- 移动互联网是一个新兴的市场，相应的安全机制发展相对较慢。
- 移动终端通常是私下和机密商业交易的载体，对黑客攻击而言是极具吸引力的目标。
- 移动网络资源更少，溢出形式的攻击将会更容易、更严重地消耗资源。
- 许多移动服务终端与其网络强耦合。恶意服务和窃取隐私可造成运营商收入受损、用户投诉和法律等方面的问题。
- 开放的/破解的移动操作系统超出了运营商的控制范围，给恶意软件的滋生提供了温床。
- 移动终端通常拥有大量的数据交换接口，如通用串行总线（USB）、安全数字（SD）卡插槽和蓝牙，因此运营商无法保证当中许多接口的安全。

为了减缓恶意软件造成的损害并跟踪威胁的来源，至关重要的是要管理好网络侧受感染的终端，而这是移动运营商的责任和义务。

ITU-T X.1126 建议书

减缓移动网络中受感染终端负面影响的导则

1 范围

本建议提供了减缓移动网络中受感染终端负面影响的导则。本建议书引入了一个框架，通过若干过程来组织导则。此外，本建议书还讨论了这些过程中的基本原则、策略和技术。

遵循本建议书并不意味着就可证明符合任何国家或地区法律、法规或政策的要求。本建议书中所述的技术方法、组织方式和程序手段并不能以任何形式保证可以达成某种等级的安全性，而使特定的国家或地区法律、法规或政策将之用于某种通信中。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书采用了下列他处定义的术语：

3.1.1 [b-ITU-T X.1245] **黑名单（blacklist）：**通信服务中有关人员或来源的一个身份清单，该清单中的人员或来源不得访问特定的通信资源。

3.1.2 [b-ITU-T X.1211] **恶意软件**：旨在专门破坏或干扰系统，攻击其保密性、完整性和/或可用性的恶意软件。

注 – 示例包括：病毒、勒索软件、间谍软件、广告软件、恐吓软件。

3.1.3 [ITU-T X.1121] **移动网络（mobile network）：**为移动终端提供无线网络访问点的网络。

3.1.4 [ITU-T X.1121] **移动终端（mobile terminal）：**具有无线网络访问功能的实体，并与移动网络相连接，以便与应用服务器或其他移动终端进行数据通信。

3.1.5 [b-ITU-T X.1244] **垃圾邮件散播（Spamming）：**由垃圾邮件发送者实施的发送垃圾邮件行为链，如收集目标名单、创建垃圾邮件、传播垃圾邮件等等。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 **僵尸网路(botnet)：**一组被盗用的计算机系统，在其所有者并不知晓的情况下，它们感染恶意软件，并出于恶意之目的而被以某种协调的方式连接在一起，用于如传播恶意软件、垃圾邮件或者发起攻击等。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

App 运行于移动终端中的应用程序

API 应用程序编程接口

C&C 指挥和控制

DDoS 分布式拒绝服务

GGSN 网关通用分组无线业务支持节点

IP 网际协议

MMS 多媒体消息服务

MMSC 多媒体信息服务中心

SD 安全数字

SIM 用户识别模块

SMS 短消息服务

SMSC 短消息服务中心

URL 统一资源定位符

USB 通用串行总线

VAS 增值服务

WAP 无线应用协议

5 惯例

无。

6 框架和过程

在大多数情况下，在被恶意软件感染后，大多数移动终端仍能继续访问网络以及像往常一样使用各种各样的服务，并开始对移动网络和服务产生负面的影响，而用户对此可能并意识不到。移动运营商必然会意识到被感染了，并对受感染的终端采取适当的遏制措施，以便可以稳定地保持其网络和服务的功能，并通过保护其用户的利益而维持其信誉。图1描述了一个用于减缓受感染终端负面影响的框架，当中包括三种类型的角色：运营商、用户和其他组织。在该框架中，运营商发挥着关键性的作用，其工作可以分为三个过程：发现、治理和信息共享。为了支持全部这三个过程，在该框架中涉及到了恶意软件和源数据库问题。考虑到在其运营的各个成员国中的国家法律和监管义务，运营商在该框架中采用了这些过程。

三个角色之间存在以下关系：运营商发现和治理网络侧用户终端的异常情况；而后告知用户关于这些异常可能造成的威胁。此外，运营商也可以与合作的运营商和组织共享关于恶意软件的信息。

在发现过程中，可对运行于移动终端中的应用程序样例（应用程序）和报告的攻击报告进行收集，并对之进行分析，以便发现移动网络中存在的异常情况。在治理过程中，对出现的异常情况和受感染终端进行报告。在治理过程中，对异常情况进行验证，并提出具体的措施以减缓对用户和运营商造成的负面影响。为及时提供信息以应对或处置移动恶意软件，应建立一个信息共享过程。在信息共享过程中，与合作的运营商和组织共享关于恶意软件的信息，以提高整个行业的安全性。

恶意软件和来源数据库：贯穿所有过程，有一个关于恶意软件和来源的数据库用来存储和提供关于此类代码的知识，包括其行为模式和来源。这些知识为在三个过程中进行异常情况鉴别、受感染终端控制和恶意软件信息发布等提供支持。此外，来自发现和信息共享过程的、关于恶意软件的新知识可上传到数据库中，以便实施“实时更新”的保护。

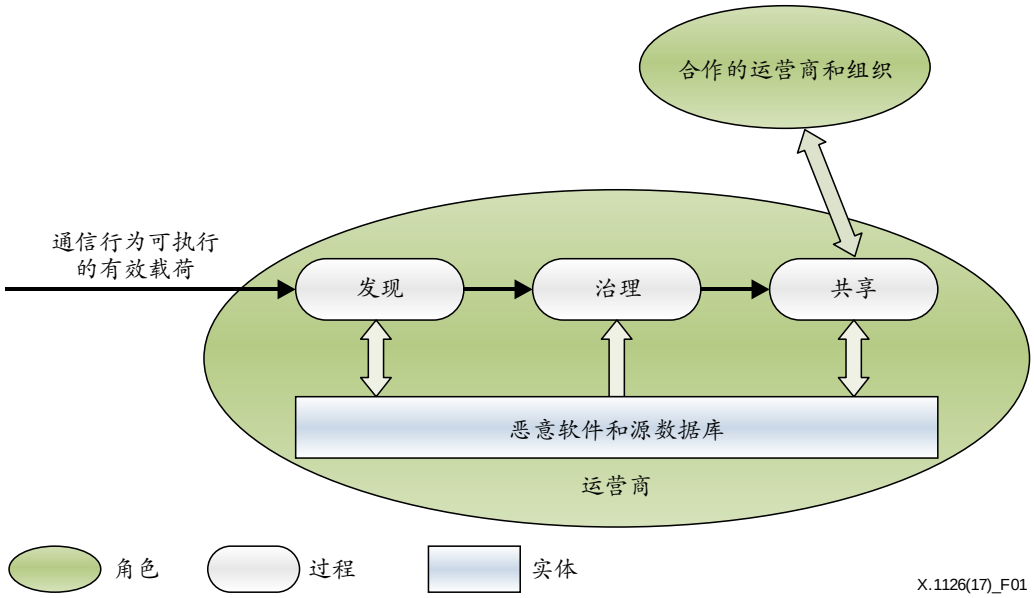

图1 – 减缓受感染终端负面影响的框架

7 发现

在发现过程中，对应用程序商店中的应用程序样例以及通过终端和通过网络元素报告的攻击报告进行收集，以便对移动网络中的异常情况做出分析，这有可能指出受感染的终端和恶意的来源，或者成为受感染终端和恶意来源的线索。图2描述了发现过程的工作流程。

本条款中所用的所有数据以及以下内容，可以从应用程序商店中的应用程序样例以及通过用户终端或通过网络元素报告的攻击报告来收集。对数据的任何使用可能与发现过程中的用户隐私有关，为此可能需要根据当地法律得到用户同意或授权。应严格保证数据只用于分析恶意软件及其相关的活动，而不会用于任何其他目的。

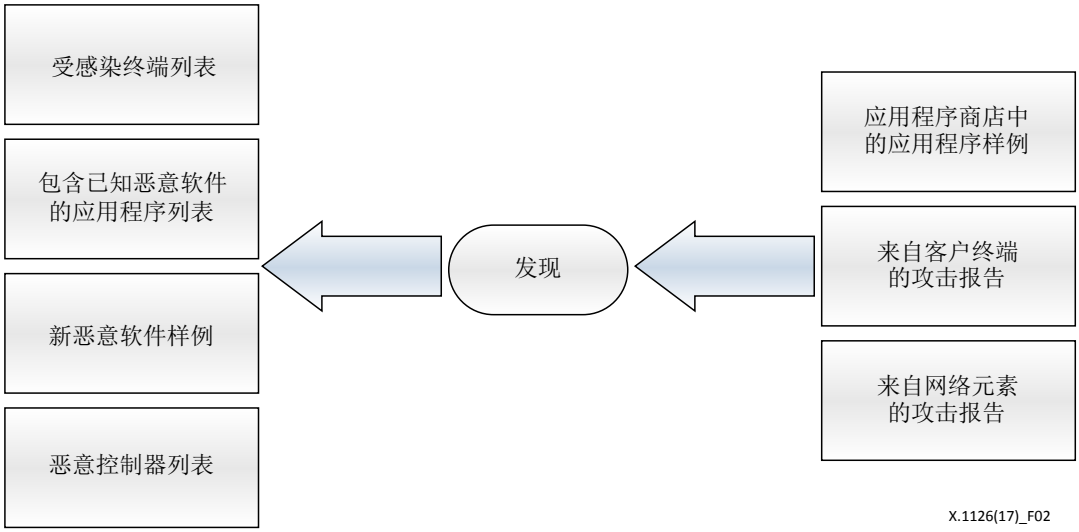

图2 – 发现过程的互动关系

7.1 收集应用程序和攻击报告

在发现过程中，针对网络异常的特性，可收集两种类型的数据：

- 来自用户终端和网络元素的攻击报告；
- 来自应用程序商店/市场的应用程序样例。

7.2 分析受感染的终端和已知的恶意软件

一些受感染的终端可能可以通过攻击报告来确定。额外的签名匹配可以帮助找到一些新的、包含已知恶意软件的应用程序。

对受感染的终端和已知的恶意软件进行分析，是用于对隐藏在网络中的恶意控制器进行定位。

应对受感染终端控制数据包中的网际协议（IP）地址进行分析，以便确定IP来源，通过它来指挥受感染的终端或收集受感染终端的状况信息。

对在应用程序中找到的已知恶意软件，应采用动态分析方法，以便检查是否对恶意控制器有过任何更改。

7.3 分析新的恶意软件

基于从应用程序商店获得的应用程序，通过行为分析、静态分析和动态分析，可以发现新的恶意软件。

7.3.1 恶意代码和可执行文件分析

静态分析：用于在句法层面理解可疑之恶意软件的方法。例如，可以通过逆向工程技术来反汇编一个移动应用程序，以获取其清单文件（包含关于应用程序访问权限的信息）和源代码。通过检查清单文件和扫描应用程序编程接口（API）调用特性，依据某些典型的检测策略，可以鉴别出大量恶意的企图与尝试：

- 如果允许任何不必要的和敏感的访问特权；
- 如果调用网络API来访问恶意的互联网来源；
- 如果调用进程API来终止某个应用程序；
- 如果调用进程API来导出联络信息至某个特定的位置；

- 如果读取安全数字（SD）（存储）卡或用户身份模块（SIM）卡的行为是异常的；
- 如果与已知的恶意统一资源定位符（URL）之间存在数据交换；
- 如果在没有用户请求的情况下存在服务订阅短消息服务（SMS）；
- 如果存在一些用于遥控移动终端的指令。

动态分析：在一个可控的（设置虚拟化的）环境中（如沙箱）运行和监控可疑之移动恶意软件的方法。以下是一些典型的检测策略：

a) 僵尸网络通信：

i) 描述：僵尸得向某个指挥和控制（C&C）服务器报告它的存在情况，以便加入僵尸网络，C&C服务器指示僵尸网络进行恶意活动。C&C服务器可以是一个万维网服务器或者移动网络中的一个终端，并且指令可以通过互联网、SMS和多媒体消息服务（MMS）服务来发布。

ii) 检测策略：

1) 大量的终端连接到一个已知的恶意主机上。

2) 一个终端定期地、长时间地连接到一个已知的恶意主机上。

3) 一个终端发送二进制SMS消息到大量的终端上。

b) 传播和垃圾邮件散播：

i) 描述：恶意软件通过各种各种的服务（互联网、MMS、SMS等）尽可能广泛地传播自身或者将垃圾邮件发送给其他用户。

ii) 检测策略：

1) 大量的终端发送相同的MMS或SMS消息（相比单向散列的消息），且其地理分布是随意的。

2) 在某段空闲时间，某个服务的量急剧飙升。

3) 进行三重调用。

4) 发送短消息服务（SMS）消息。

5) 发送多媒体消息服务（MMS）消息。

6) 如果软件调用某个已被起底的调用。

7) 如果SIM卡的信息通过软件导出到某个服务器上。

8) 如果在一段较短的时间后通过软件调用了某个恶意调用。

9) 如果诱导了任何不必要的额外下载。

10) 访问已知的恶意控制器。

c) 恶意订购和消费：

i) 描述：受感染的终端将订购增值服务（VAS）和三重调用服务，以拨打高价电话或国际电话，并发送大量的消息。用户将不会意识到这些费用。

ii) 检测策略：

1) 用户账出现不明的飙升。

2) 受感染的终端在特定的时期频繁地拨打高价电话或国际电话。

3) 大量的终端在特定的时期经常地多次发送相同的消息。

4) 终端订购三重调用服务，并频繁地使用它们，甚至时时使用它们。

d) 分布式拒绝服务（DDoS）攻击：

i) 描述：一大群终端涌入并占用移动网络的无线电资源和其他资源，从而对服务质量造成损害。

ii) 检测策略：

1) 网关GPRS支持节点（GGSN）或其他网络实体的通信流量急剧飙升，并且绝大多数的通信流量具有相同的目的地。

静态分析不适合用于隐蔽的或模糊的可疑恶意软件，动态分析不能涵盖完整的程序代码。因此，既应执行静态分析，也应执行动态分析，以便彻底了解特定的恶意软件是如何作用的。

通过静态分析和动态分析捕获到的和鉴别出的异常企图或行为，对在最新的异常情形下的行为分析而言是有用的。此外，这些鉴别出的特性也将有助于运营商发现未知的恶意URL或IP地址。

7.3.2 结合方法

因此建议将两种分析方法结合起来，以提高性能，并减少发现过程的误判。

在发现过程中，可以生成各种各样的输出结果，以支持以下治理过程。发现过程的输出结果应包括但不限于：

- 受感染终端的清单；
- 包含已知的恶意软件的应用程序样例；
- 新的恶意软件样例；
- 恶意控制器的清单。

上面的信息对运营商在以下过程中采取适当措施而言至关重要。

8 治理

在治理过程中，自动地或半自动地对发现过程的输出结果进行分析和验证。然后，依据异常情况的严重程度采取相应的治理措施。图3描述了治理过程与其他网络和服务实体之间的互动关系。

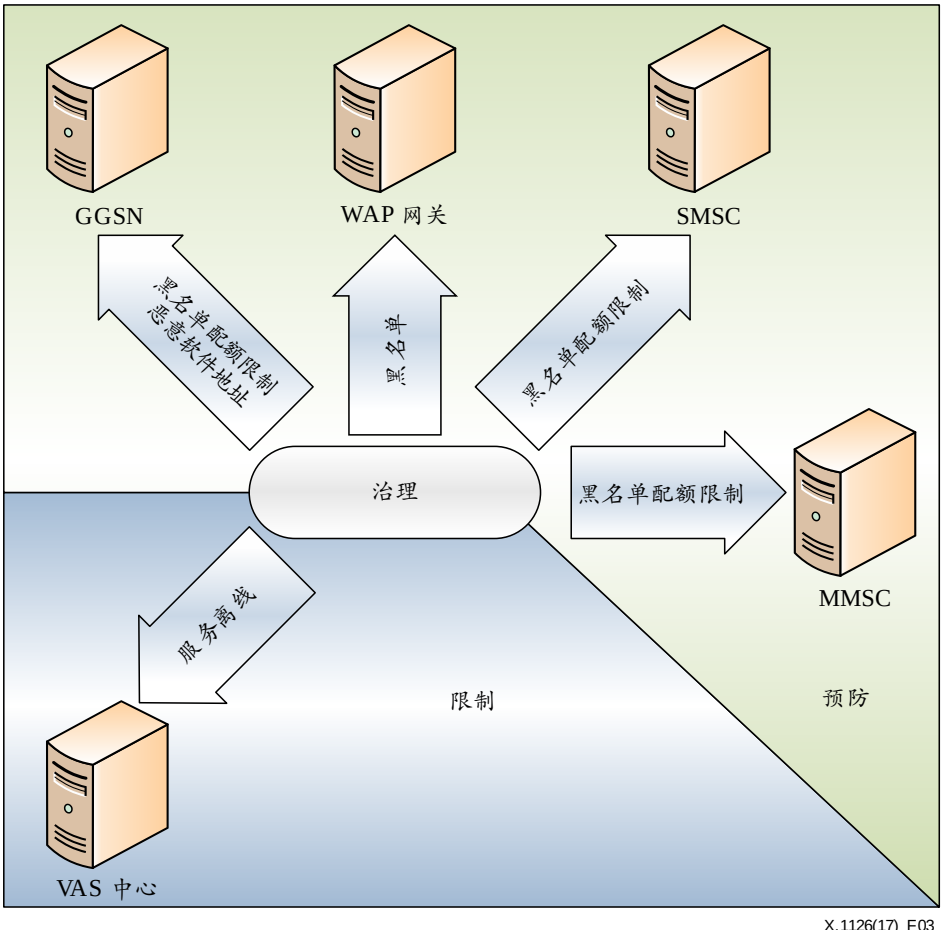

图3 – 治理过程的互动关系

8.1 治理措施

有两种措施与不同的异常情况严重程度有关：预防和限制，这两种措施都只能利用支持平台的网络实体和服务的功能。

- 预防：如果异常情况的严重程度属于中等，并且在不中断用户服务的情况下就能得到控制，那么可采取预防措施来处置该问题。
- 限制：如果预防措施不起作用，并且用户已经遭受巨大的财富损失，那么将采取限制措施，有选择地或完全地暂停受影响的服务。

8.2 预防

8.2.1 黑名单

当异常情况是由恶意控制器触发而出现的时候，可将控制器添加至黑名单中。而后，任何至/自该控制器的后续请求都将被阻断。有许多网络实体，如GGSN、无线应用协议（WAP）网关、多媒体消息服务中心（MMSC）等，都支持黑名单功能。可以保存多个黑名单，以便阻断不同类型的恶意控制器，如恶意网站的域名、C&C服务器的IP地址等。注意：将定期对黑名单中的来源进行确认和更新，以免阻断合法的来源。

GGSN可阻断任何与下载包含恶意软件的应用程序有关的地址。

8.2.2 配额限制

当垃圾邮件散播行为是引起网络异常的主要原因时，如DDOS攻击，那么可采用配额限制方法来减缓扩散的速度。配额限制定义了一个关于可在某段时间周期内（例如，一个月）发送的、最大消息数量的阈值，以便全面保证任何终端的基本/应急通信能力。当消息数量超过该阈值时，将不再允许发送任何更多的消息。

8.3 限制

8.3.1 运营商业务下线

如果一个恶意控制器位于某个运营商的服务中，这可能是由黑客行为引起的，那么运营商可以行使权利和义务来暂时下线自己的服务，并必要时，可以依据应急通信义务启用备份服务。

9 信息共享

治理不能作为最终目标，它只是力图尽可能减少对用户和网络的负面影响。最终的目标是让事情恢复正常，并力图防止出现更大的感染。因此，信息共享过程对整个框架的完美运转而言是非常重要的。

为提高行业福利，只在运营商之间共享有关恶意软件的样例。

注意：信息共享过程应符合当地法律和订购合同的要求。

参考资料

[b-ITU-T X.1121] ITU-T X.1121建议书（2004），移动端到端数据通信安全技术框架。

[b-ITU-T X.1211] ITU-T X.1211建议书（2014），防范网络攻击的技术。

[b-ITU-T X.1244] ITU-T X.1244建议书（2008），IP多媒体应用反垃圾邮件概述。

[b-ITU-T X.1245] ITU-T X.1245建议书（2010），IP多媒体应用反垃圾邮件框架。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦