针对提高域名系统 (DNS) 安全性、稳定性和适应性的提议行动方案

提供者

互联网名称与数字地址分配机构
(ICANN)

征求公众意见

2010 年 2 月 12 日

针对提高域名系统 (DNS) 安全性、稳定性和适应性的提议行动方案

1. 概述

本文介绍了与域名系统 (DNS) 的安全性、稳定性和适应性相关的两个战略行动方案的理论依据、关键特点和预计成本。互联网名称与数字地址分配机构 (ICANN) 认为，对于履行其章程《2009 年承诺确认书》和 2010 – 2013 年 ICANN 战略计划赋予的职责，这两个战略行动方案是不可或缺的。本文为多利益主体对这些提议行动方案的讨论、ICANN 就实现提议功能所承担的责任，以及社区继续组织工作以向这些行动方案提供支持的可能方式提供了依据。本文还确定了高级工作人员和资源的含义，但未分析这些行动方案的资金替代方案。

注意： 这些作为工作提议的行动方案超出了为在内罗毕会议上展开讨论而发表的 2011 财年 ICANN 运营计划和预算框架中所确定的行动方案。

2. 假设

2.1 域名系统已成为增强互联网服务的最基本、最基础的服务内容。域名系统 (DNS) 为网络用户提供了名称解析，还为电子邮件、文本消息、支持互联网功能的语音及其他关键互联网服务和协议奠定了基础。但是也要考虑到，DNS 存在于威胁和风险日益增加的环境中。此系统的技术运营要承受一系列的攻击，例如分布式拒绝服务 (DDoS) 对高级别权威名称服务器和解析器（包括根名称服务器）的攻击；由安全研究人员 Dan Kaminsky 所描述的会影响 DNS 解析完整性的缓存感染病毒攻击；以及包括允许恶意攻击以误导和滥用 DNS 服务的社会工程在内的其他方法。此外，破坏者和犯罪分子可利用用户对 DNS 的依赖，并通过多种方式使用此系统来进行广泛的恶意活动。

2.2 目前，提供 DNS 服务的运营商团体与供应商、安全研究人员、执法机构和响应团队积极合作，以便有针对性地对随时出现的威胁作出反应。DNS 社区制定了行动方案来提高信息共享，以确定恶意活动并加强与 DDoS 和其他全系统攻击有关的合作。这些合作通常涉及 DNS 和安全社区成员自愿为应对随时出现的情况共同努力。去年已制定了关于应对及减少系统性 DNS 风险的多项行动倡议。[1] 这些行动倡议的频率及严重性揭示了对全系统风险评估、应急计划和常备应急能力的需求与日俱增。

[1] 请参见 http://www.enisa.europa.eu/media/press-releases/improving-resilience-3-tips、http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks 和 http://www.it-scc.org/documents/itscc/IT-SCC_ITSRA_Release_08_21_09_clean_final2.pdf。

2.3 当前针对解决 DNS 的一系列威胁和风险所做的努力尚未得到系统性的关注。在运营层面上，DNS 中资源充足、了解安全的运营商为了解威胁及采取行动以减少自身及客户的风险开发了强大的机制。然而，在该领域的合作通常未扩展到能力较弱且资金不足的 DNS 运营商，以及未意识到威胁和风险并且在意识到安全性、稳定性和适应性的此类威胁时无法充分做出响应的其他利益主体。此外，现有的努力已表明需要对监控、响应和补救持续关注，以便应对无法轻松通过本地化技术修复就能消除的威胁。在更高层面上，DNS 缺少与风险评估、应急计划和演习以及专门的持续响应中关键功能相关的责任制重点。此类活动必须全盘考虑 DNS，并对各个组成部分和运营商的需求做出响应。

2.4 从根本上来看，这些类型的功能不能完全依赖于志愿者在没有任何专门的组织支持、完善的运营方法和长期资源承诺的情况下所做的努力。为了确保 DNS 的稳定性和适应性，所做的努力必须按照对全职员工的投资及支持所需类似级别的通讯架构的其他关键方面，达到效力和责任制级别。

3. 互联网名称与数字地址分配机构 (ICANN) 的角色和职责

3.1 DNS 必须以安全、稳定且灵活的方式运营。ICANN 已做出大量承诺，保证尽心竭力来实现这一目标。ICANN 章程的第 I 条规定：“互联网名称与数字地址分配机构 [ICANN] 的使命是，对全球互联网的唯一标识符系统进行总体协调，特别是确保互联网唯一标识符系统稳定安全地运作。”《2009 年承诺确认书》 (http://icann.org/en/announcements/announcement-30sep09-en.htm) 宣称，DNS 作为互联网环境中的关键功能，必须对与运行相关的风险进行相应管理。ICANN 已承诺“保持 DNS 的安全性、稳定性和适应性。” 此外，《承诺确认书》还要求 ICANN 确定当前及未来的威胁并制定相应的应急计划。

3.2 ICANN 的这些承诺的含义非常明确。《承诺确认书》要求 ICANN 积极开展合作，以确定并减少整个分发 DNS 系统中安全性和适应性的风险，合作对象包括运营及使用 DNS 服务的大量利益主体。[2] 由于 DNS 的性质，根服务器系统以及顶级域的可靠且灵活运营必须是 ICANN 的首要工作重点。随着使用的自然增加而增长的 DNS、新技术的引入以及建立新 TLD（包括使用国际化域名的 TLD）的提议，进一步要求 ICANN 了解并寻求降低系统的风险。需要注意的是，自创办以来，ICANN 一直寻求提高 DNS 的安全性、稳定性和适应性。ICANN *针对增强互联网安全性、稳定性和适应性的计划* (http://www.icann.org/en/announcements/announcement-2-21may09-en.htm) 可以应对大量现有项目和活动。本文中列出的行动方案要求 ICANN 必须做出进一步努力以履行这些承诺。

[2] 由于 ICANN 计划履行其管理 DNS 安全性、稳定性和适应性风险的角色，因此它不解决网络战争、间谍活动或互联网上托管的内容地址控制领域中与各州之间国家安全竞争有关的问题。 请参见 http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf。

3.3 提高系统性认识的紧迫性以及减少 DNS 风险并实现其承诺要求 ICANN 与 DNS 社区合作，以便以过去的工作和当前的合作为基础，开展进一步的工作。为此，《2010 – 2013 年 ICANN 战略计划》将提高 DNS 的稳定性、安全性和适应性确定为 ICANN 在此期间的四个工作重点之一。战略计划具体满足了 ICANN 为域名系统计算机紧急响应团队 (DNS-CERT) 建立方法以及针对 NDS 的应急计划和演习的要求。ICANN 寻求不断进步，以确保建立可评估风险、对潜在的威胁计划及演习紧急事务并组织协调合作事件响应能力的全系统方法，从而提高 DNS 系统的整体安全性、稳定性和适应性。ICANN 还计划努力提高全系统衡量标准，从而使 DNS 社区能够清楚地了解 DNS 的安全性、稳定性和适应性并预测和有效应对挑战。

3.4 下文所列出的行动方案的预期效用及成功运营将需要社区的支持和参与。与实施这些行动方案有关的社区审查、反馈及计划将与 ICANN 的运营计划和预算流程整合。

4. DNS 运营的风险

4.1 跨入 2010 年后，互联网生态系统仍将生机勃勃。互联网上的活动将越来越多地反映全部人类动机和行为。在某种程度上，此类活动将反映使互联网能够在其边缘成功实现创新、允许以全局公用的方式进行通信、创新和交易的公开性质。生态系统还受到由各种参与者所开展的级别不断提高的恶意活动的威胁，有迹象充分表明，犯罪组织的参与正在快速增长。威胁前景展望包括：欺诈、敲诈和其他非法在线活动（这些活动会打击用户对基于互联网的服务的信心）；拒绝服务 (DDoS) 攻击；以及扰乱互联网基础结构的其他破坏性活动。尤其是恶意参与者能够对 DNS 自身的功能进行攻击并能够轻易且频繁地使用名称解析和注册服务进行一系列的恶意或犯罪活动，这表示互联网正常运营的风险不断增加，让人开始怀疑互联网作为全球交流平台的完整性和可靠性。

4.2 安全性、稳定性和适应性风险的三个主要类别包括： 恶意活动（对 DNS 进行攻击或利用名称解析或注册系统进行攻击）、DNS 稳定性的技术风险以及与 DNS 有关的组织风险。

4.2.1 恶意活动风险

4.2.1.1 互联网名称与数字分配机构 (ICANN) 要考虑的主要核心风险是 DNS 解析名称并促进整个互联网中各种交易的可用性。可用性面临的最大威胁的形式可以是 DoS 对系统各个级别上正在运营的 DNS 服务进行攻击。DoS 攻击的影响取决于目标服务的类型和复杂程度以及攻击的流量。在过去的十年中，根服务器以及顶级域 (TLD) 的运营曾多次受到直接攻击。以下是四个最突出的实例： 1) 2002 年 10 月 21 日，首次记录了对十三个 NDS 根服务器的协同攻击的案例 (http://d.root-servers.org/october21.txt)；2) 2006 年 2 月，关键 TLD 名称服务提供商对名称服务器发起了攻击 (http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf)；3) 2007 年 2 月，对十三个 DNS 根服务器中的六个发起了攻击 (http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf)；4) 最近，2009 年 12 月，对 NeuStar 的 UltraDNS 服务攻击影响许多电子商务网站的同时新闻中再次报道了 DoS 对 DNS 提供商发起攻击 (http://www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html)。攻击的历史记录表明了那些进行攻击的人可以获得持续增加的资源以及操纵者的复杂程度。

4.2.1.2 在提供配置带宽以处理 DDoS 及建立和部署技术及方法方面，正在做出重要努力以减少这些风险，例如任播，即将数据路由到最佳或最近目的地。以部署任播解决方案为例，DNS 根服务器系统已从十三个位置（系统）增加到二百多个位置（有关详细信息，请参见 http://www.root-servers-org）。随着诸如 DNS 运营分析和研究中心 (DNS-OARC) (http://www.dns-oarc.org)、注册机构互联网安全组 (RISG) (http://registrysafety.org/website/) 等组织的建立以及对于了解与 DNS 有关的风险所做的努力（如 DNS 安全性、稳定性及灵活性座谈会）(http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf)，DNS 运营商之间的计划和合作级别也不断提高。然而，由于越来越多的 bot 网在犯罪分子及其他恶意参与者的控制之下，这会在复杂程度和规模方面都有进行非常重要攻击的风险，因此威胁也在增加。为此类破坏做计划时，必须也要处理由于对为 DNS 提供电力和互联网路由的系统进行的恶意攻击而使 DNS 服务中断这一可能性。

4.2.1.3 由于 DNS 运营的公开和分布式性质，以及名称服务器和解析器的广泛分布式管理，使用户易受许多其他风险的威胁。DNS 协议（不使用安全扩展）易受采用查询*误导*的攻击。具体而言，攻击会返回错误信息对 DNS 查询做出回应（*病毒*或*网址嫁接*）或不同于域名机构本意的信息（重定向或响应修改）。此类攻击采用以下各种方式令 DNS 用户受骗： 使用户进入具有欺诈性内容或恶意代码的网站、使电子邮件看似来自于欺诈源等等。进行攻击的技术可允许 DNS 缓存的系统性病毒进入，因此互联网流量的重定向为可能会对整个 DNS 的完整性构成风险的恶意活动提供了机会。

4.2.1.4 域名注册服务为破坏者提供了另一个攻击平台。攻击者将攻击注册管理人或域名注册人(可以利用社会工程手段的员工）的技术（网站漏洞）或运营弱点，以获得对域名注册帐户的未授权控制（有关详细信息，请参见 SAC040 http://www.icann.org/en/committees/security/sac040.pdf）。控制劫持的注册账户之后，攻击者可能会将劫持帐户中所有域的 DNS 配置更改为指向受其控制的名称服务器，从而可以控制对受损域的网站、电子邮件及其他互联网应用程序的名称解析。此类域名或帐户劫持攻击将用于破坏网站、中断由注册人提供的电子邮件或其他服务，或者获取敏感性或个人信息。

4.2.1.5 尽管 DNS 旨在为互联网用户提供服务，但非常遗憾的是，DNS 仍会受到破坏者的攻击，助长了大量犯罪行为和滥用。这一意外结果是 DNS 受到攻击从而助长恶意活动的最好例证，通称为*网络钓鱼*。仿冒者注册专门支持从受损或 *bot* 计算机的网络中发起的攻击的域名，称为 *bot 网*。攻击者通常使用其中某些恶意域名来运行*犯罪 DNS*，它是 DNS 解析器的集合专用于编程和部署以解析由网络钓鱼受害者提出的 DNS 查询。其他恶意域名用于托管假冒网站。回应受害者针对看似合法的金融机构、电子商务、慈善团体、政府机构或类似实体域名的 DNS 查询，让这些不知情的用户进入欺诈性或假冒网站。与通常在金融机构、电子商务、慈善团体或政府机构的合法网站上一样，受害者无意中在此假冒网站上互动交流。然而这些恶意网站旨在盗取他人的身份、银行帐户和信用卡信息、向受害者销售非法或伪造产品、诈骗慈善团体等等。[3]

[3] 美国国土安全部、信息技术政府协调委员会。2009 年信息技术部门基线风险评估。华盛顿特区： 政府印刷局，第 32–33 页。

4.2.1.6 DNS 在使 *bot 网可供出租*方面的作用也越来越突出，对在蓬勃发展的地下经济中提供服务的网络进行攻击。Bot 网由成百上千甚至几百万台受到远程控制的受损计算机 (bot) 组成，可执行多种类型的恶意攻击（如 DDoS）或支持犯罪活动（人口贩卖、非法药品销售、垃圾邮件等等）。为了有效控制 bot 并对安全工作者和执法机构的对策保持相当大的适应性，攻击者会对 bot 进行编程以使用 DNS 确定命令和控制的地址或者向 bot 发布命令的*会合点*。最近，某些恶意软件（如 Conficker 恶意软件的变种）已使用某些方法来寻求依赖预定的几组域名作为控制 bot 的关键方面。

4.2.2 技术风险

4.2.2.1 广泛使用有问题的运营实践会导致服务中断，进行技术更改会导致便于破坏者或犯罪分子进行恶意活动的意外漏洞，DNS 的运营或完整性都会受到不利影响。属于后一种问题的实例及当前解决此类问题的主要反应形式出现于 2008 年。安全专家 Daniel Kaminsky 发现了 DNS 协议中的严重漏洞，随后公开表明名为 DNS 响应修改的做法会受到攻击者的攻击，使其完全可以在主要公司的管理范围之外使用虚拟主机服务劫持这些主要公司的网站。互联网名称与数字地址分配机构 (ICANN) 安全性和稳定性咨询委员会 (SSAC) 稍后在社区中发布了潜在威胁 DNS 响应修改的咨询警告 (http://www.icann.org/en/committees/security/ sac032.pdf)。临时特别系统投入使用，从而使 DNS 运营商和用户能够测试其系统的漏洞并采取预防或补救措施。ICANN 社区已开始并继续制定多个行动方案，这些行动方案可能有助于更协调地披露以及更有组织的响应与 DNS 有关的这些威胁。其中包括 ICANN 与合作伙伴一起进行年度研讨会，把专家召集在一起研究威胁前景展望，集体评估风险并就如何消除风险提出建议。第一次研讨会于 2009 年 2 月与乔治亚技术信息安全中心 (GTISC) 联合举办。

4.2.2.2 如果对 DNS 所做的技术更改更改了系统的行为或者导致需要对当前或计划容量进行实质性更改的流量负载，DNS 的运营也会受到不利影响。为了降低采用会破坏 TLD 级别上 DNS 安全性和稳定性的运营实践的可能性，ICANN 董事会于 2009 年实施了一些步骤，以禁止基于风险使用重定向，此实践对由安全性和稳定性咨询委员会所规定的 DNS 稳定性构成威胁 (SAC041 http://www.icann.org/en/committees/security/sac041.pdf)。[4] DNS 社区将于 2010 年继续全面审核由对根 DNS 级别进行的一系列提议的更改而导致的潜在影响： DNS 安全扩展 (DNSSEC) 的实施、IPv6 的实施以及将 IPv6 粘附记录添加到根区域文件的需要、快速跟踪引入使国际化域名 (IDN) 标签可在 DNS 顶级上使用，以及引入新 TLD。

4.2.3 组织故障

4.2.3.1 在 DNS 运营的有效运行中发挥关键作用的潜在组织故障也构成重要风险类别。在 DNS 的核心，互联网名称与数字地址分配机构 (ICANN)、根服务器运营商、顶级域名 (TLD) 注册机构和注册管理人可在无中断的情况下提供服务，这一点对 DNS 的总体安全性和稳定性至关重要。其中每个实体单独负责其各自的财务自生能力、业务连续性和风险管理，但在系统级别上，当组织可以不再行使其职能时必须对应急响应做出规定，在适当时，也要对服务的恢复、永久化或重组方式做出规定，以确保 DNS 运营继续有效并保护注册人。

[4] 美国国土安全部、信息技术政府协调委员会。 2009. 信息技术部门基线风险评估。华盛顿特区： 政府印刷局，第 32–33 页。

4.2.4. 衡量风险和安全性、稳定性以及适应性

4.2.4.1 目前，针对与安全性、稳定性和适应性有关的正确措施和整个系统可接受的性能水平没有完全达成共识。各个运营商和独立的研究人员已对 DNS 的各个方面进行了衡量，但到目前为止，在制定和实施标准、全系统标准或可接受的服务水平方面没有多大进展。在努力提高与 DNS 安全性、稳定性和适应性有关的风险管理时，必须将衡量这些特征和评估的改进能力以及计划和资源的投资效用作为指导。

4.2.4.2 改进这种情况的关键因素是确保正确检测和衡量 DNS 运营的组成部分。2009 年根服务器研究团队 (RSST) 关于调整根区域的报告 (http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf) 要求根据根服务器系统“建立用于检测和减少出现的风险的有效机制”。衡量标准的建立以及检测的确构成一些有趣的挑战。尤其是 DNS 的分布式性质要求建立合作衡量模型，这需要众多参与者和组织的参与。各种组织都在研究互联网预警系统的主题，其中包括欧洲网络与信息安全局 (ENISA)，它将于 2010 年 3 月就互联网预警和网络智能这一主题举办首次研讨会 (http://www.enisa.europa.eu/events/ee/ EWNI2010)。ICANN 与京都大学将于 2010 年 2 月就 DNS 的安全性、稳定性和适应性这一主题联合举办第二届全球研讨会，将对衡量标准进行重点讨论。ICANN 计划鼓励开展一些可改进对于如何衡量 DNS 风险的了解情况以及可提高系统的运行状况、安全性、稳定性和适应性的活动并参与到其中，作为在建立有效风险评估、应急计划/演习和响应能力方面的基本推动者。

5. 战略行动方案

5.1 此处提出的两个行动方案满足了实现 ICANN 所需功能从而履行其在早期确定的安全性、稳定性和适应性承诺这一关键需求。如在开始时所述，本文旨在为多利益主体对这些提议行动方案的讨论、ICANN 就实现提议功能所承担的责任，以及社区继续组织工作以向这些行动方案提供支持的可能方式提供了依据。本文还确定了高级工作人员和资源的含义，但未分析这些行动方案的资金替代方案。本文未预先假定 ICANN 将为这些行动方案提供资金和人员。

5.2 本文中附带的 DNS-CERT 商务案例更详细地说明了关于需要建立 DNS-CERT 的行动方案 2。

5.1 行动方案 1 – 全系统 DNS 风险分析、应急计划和演习

5.1.1 按照《承诺确认书》的要求，ICANN 将与 DNS 社区服务以主动了解 DNS 的主要风险，包括分析新出现的威胁和风险。分析完这些风险后，DNS 社区必须确定全系统 DNS 安全性、稳定性和适应性的应急计划最大关注点，并确保减少已确定风险的计划工作已经就位。ICANN 认为自己在使全系统应急计划和演习成为《承诺确认书》中所规定的职责的一部分方面起重要作用。此类主动计划是对响应能力的补充，除了将组织作为自然中心以支持应急计划和演习计划之外，它还可由 DNS-CERT 提供。

5.1.2 此行动方案的第一个方面是制定基于社区的风险分析方法，其中包括已接受的 DNS 分析框架和关于衡量风险的改进方法。这项工作将包括建立执行常规 DNS 风险评估和风险缓解提议的方法。这项工作将建立在 2010 年 DNS 安全性、稳定性和适应性研讨会以及 DNS-OARC、ENISA 和其他组织的工作基础之上。

5.1.3 此行动方案的另一个方面是加强整个社区在应急计划范围内的合作，并使用该计划作为建立响应能力工作的指导。应急计划的依据应开始于在全系统 DNS 风险框架（确定了 DNS 和关键情况下的顶级风险）方面达成的共识。这项工作建立在现有工作的基础之上，如通过那些关心重要基础结构保护的公私合作机构开展的工作，例如美国信息技术部门协调委员会和 ENISA 以及那些作为 DNS 运营社区的一部分开展工作的组织（如 DNS-OARC 和荷兰 [NL] 网络实验室）。此提议行动方案还会设想与新出现的根服务器系统信息共享机制和 TLD 注册运营商的紧密合作。对于风险和关键紧急事务的分析将用于评估当前响应机制的充分性，确定需要采取行动的缺陷，以及为已确定的紧急事务制定应急计划。这项工作应得到整个社区范围内的专家咨询/工作常设小组的支持。ICANN 将假设有责任为小组提供支持并为社区审查制定行动计划，构成对 ICANN 对其安全性、稳定性和适应性以及运营计划预算年度周期的投入。

5.1.4 一旦建立应急计划，将有必要使用全系统 DNS 训练计划，以确保响应能力的评估和赤字的确定。[5] 使用 DNS-CERT 和应急计划的同时，训练计划的开发还需要建立在现有活动和相关努力（例如作为较大计划子元素的现有 TLD 应急训练）的基础上。训练计划开发的目标应该是启动活动计划，该计划可以最终导致以关键紧急事务的响应为重点的一年两度的全系统 DNS 训练。此外，该计划应该包括与其他训练计划（例如多国家/地区网络风暴训练系列和其他国际多利益主体训练）的整合。正如《承诺确认书》中所规定，ICANN 有责任支持全社群都能使用此类计划，从而使计划的子元素能够更加适合应用并精心编排一年两度的全系统 DNS 训练。

5.1.1 具体的建议步骤

5.1.1.1 建立 DNS 风险评估和应急计划专家咨询小组。该小组将由来自 DNS 运作和网络安全社群的专家组成。ICANN 将为小组提供人力支持。该小组初步的工作重点是，在 2010 年第三季度之前为系统性 DNS 风险和关键现有风险的确定建立社群能够接纳的框架。此外，小组还将在 2010 年 DNS SSR 标准研讨会的基础上开展工作，以便在 2011 年初建立一个社群能够接纳的框架，以便用于测量 DNS 的牢靠性、安全性、稳定性和适应性。该小组还将负责在 2011 年第二季度之前建立起基本应急计划方案。2011 年第三季度发布第一份报告后，该小组将实施年度 DNS 风险和缓解报告。

5.1.1.2 建立 DNS 根系统共享机制将需要与根服务器运营商社群和建立在 2009 根域调整研究建议基础上的其他根服务器社群共同协作。成立由 ICANN 提供人员支持的工作小组是为了确定功能和性能监控的需求。其关键功能将包括成熟的 DNS 根系统建模、根系统相关机构的改良信息共享、必要感应器的潜在部署和用于评估当前 DNS 根系统牢靠性和为新出现的问题提供警告的专门的分析支持。这些努力将与社群一起执行和部署感应器，并测量那些可以概览根服务器和 TLD 系统的标准以及 TLD 系统的运转。该努力需要与 TLD 运营商、根服务器运营商、NTIA、ICANN 以及与核心 DNS 基础设施运行和管理相关的其他机构协作。T 我们预计，随着 DNS-CERT 的发展，该系统将以相互支持的方式建立。

[5] 此类计划对 DNS 的要求在《DHS IT 领域风险评估》中有明确规定。

5.1.1.3 根服务器运营商应急计划和训练的持续支持。随着 2010 年下半年通讯训练和初始桌面训练的成功，ICANN 将与运营商一起安排接下来的工作，以便为应急计划和基于方案的训练制定计划性的方法。ICANN 将部署可以在其本身的根服务器运行中使用的系统中补充和促进现有系统的通讯功能。

5.1.1.4 TLD 连续性计划和训练的持续完善。随着用于新通用顶级域 (gTLD) 处理的数据托管规范的发展，ICANN 和 TLD 注册运营商将在 2010 年全年乃至 2011 年执行数据托管测试。其他训练将以 ICANN 和 TLD 注册运营商之间的通讯和危机响应元素为重点进行计划安排。

5.1.1.5 启动 DNS 全局训练和评估计划的开发。此类计划将包括使用现有的努力并要求广泛的利益主体（例如与 DNS 运行相关的机构、DNS 供应商和用户社群以及更为广泛的网络安全社群）参与其中。该计划还将涉及交叉项目的理解和利用，这些项目与其他网络安全以及相关训练和评估计划交叉在一起。截至 2010 年底，该项努力将对现有努力的性质和适合性进行评估并确定它们的关键差距。到 2011 年中，我们将为社群评鉴开发一套建议性 DNS 训练计划概念文件。此外，ICANN 将在 2011 年下半年主办一次全系统的小规模训练，以便为那些下决心要建立长期计划和执行过程的利益主体树立自愿参与的原型。该原型训练的计划将从 2010 年开始。ICANN 的员工和 DNS 社群的其他成员将参加这个 Cyber Storm III 多边训练，并且有可能参加其他的国际训练。

5.1.2 资源预测

5.1.2.1 为以下五个专职人员职位预测需求：

- 高级协调员、风险评估、应急计划和训练计划
- 应急计划协调员
- 训练和评估计划协调员
- 训练规划者
- 系统分析员/建模专家、根系统信息共享系统

5.1.2.2 支持需求将包括根服务器系统信息共享的需求定义；对风险分析和根服务器信息共享的支持；基础设施和相关成本（包括用于建模、根服务器系统信息共享和通讯系统以及感应器系统的原型部署的许可和软件/硬件支持）；工作小组和员工以及提供实体设备和 IT 支持的其他员工的差旅和会议费用。

5.1.2.3 从 2010 年 7 月到 2011 年 6 月，为了支持该努力，预计我们将提供大约 1,250,000 美元用于支付员工工资，850,000 美元用于其他支持。该方案首年的年度总计划开支将为 2,100,000 美元。

5.1.2.4 **假设：**风险分析将利用来自 DNS-CERT 的威胁信息和分析。根服务器信息共享系统将利用专为 DNS CERT 开发的 Web 2.0 门户来支持信息共享。

5.2 新方案 2 - DNS-CERT

5.2.1 除了主动的风险评估、应急计划和训练，DNS 社群还需要有效的、可运行的、全系统的响应功能，以便充分地应对安全性、稳定性和适应性的挑战。对 DNS 的大规模协同攻击会带来重大的经济和政治后果，但是，在 DNS 中并没有可以进行技术和政策协调的事件管理核心联系人，该联系人可以确定和协调对此类事件的响应。2009 年，为了解决这项不足，全球 DNS 安全性、稳定性及灵活性座谈会对 DNS 及其建议行动之间的安全响应差距作出了明确规定。此外，许多 DNS 运营商并不具备充分的资源，以至于在开发强大的安全性和适应性方面受到种种限制。此类机构要么不知道去哪里寻求援助，要么遇到语言或地理障碍，从而对援助造成了阻碍。此类机构可能会成为整个 DNS 系统中易受伤害或攻击的薄弱点。ICANN 相信，作为核心联系人，DNS-CERT 必须为 DNS 提供技术和政策协调并与 DNS 社群一起发挥作用，来确定和协调对全球 DNS 事件的响应。

5.2.2 为了加强对处境的认识，DNS-CERT 将会与 DNS 一起协调现有的努力，以便整个社群随时都能够获得正确的专业知识。此类努力中关键的利益主体可以是 DNS 运营商和用户、供应商、安全研究人员和事件响应者。DNS-CERT 可以利用大量的现有努力，以便在 DNS 中确定威胁、共享信息和设备响应。DNS-CERT 活动可以为这些现有努力的合作和协调提供帮助，并为目前涉及不到的领域提供服务，或者与那些并未参与这些努力的利益主体一起为现有的努力提供帮助。DNS-CERT 可以与 ICANN 支持一起启动，但具体的组织结构和资源配置模式将通过与社群的对话确定。在这个方面，对 DNS-CERT 的监督将通过基于赞助商的董事会来执行，该董事会可以确保 CERT 赞助者的责任机制，同时还可以根据由机构担任的利益主体的需求，评估 DNS-CERT 的活动。DNS CERT 的运作将由管理和技术人员组成的核心团队进行监督，并通过由虚拟专业知识增强装置组成的扩展团队进行协助。虽然这些增强装置以地理分散的方式进行运作，它们却能够提供有形的支持。

5.2.3 DNS-CERT 既能为它的赞助者提供主动式服务（即威胁分析、DNS 牢靠性和安全性监控、处境认识和信息共享），也能提供被动式服务（即 365 x 24 x 7 联系人、事件处理协调、漏洞管理支持和安全咨询服务）。此种方式相当重要是因为以下两个原因： （1）主动威胁展望信息可以帮助 DNS 社群通过培训和训练为威胁制定计划；同时，（2）被动事件处理服务可以协助参与机构（例如来自全球欠发达地区的注册商）解决重大的资源限制。威胁信息和分析还将满足系统性 DNS 风险确定的计划建立的需要并为新方案 1 提供功能分析。DNS-CERT 能够提供的核心功能的功能性需求定义将通过基于社群的分析发生，该分析将涉及 DNS-CERT 的利益主体和潜在合作者。

5.2.2 资源预测

5.2.2.1 根据对具有相似责任规模和水平的国家/地区 CERT 团队的评估，我们相信，通过大约由 15 人（包括一名负责人、两名高级经理、十人组成的事件管理团队以及员工管理人员/法律支持人员）组成的员工队伍的年度预算，DNS-CERT 能够在初始阶段正常运转。计划员工支出为 2,600,000 美元。用于员工差旅、通信和分析工具、实体设备和 IT 支持的支持支出预计为 1,600,000 美元。用于该新方案的第一年的预计总支出为 4,200,000 美元。详细信息，由本文件附带的“DNS-CERT 业务案例”提供。

6. 结论

DNS 所面临的安全性、稳定性和适应性挑战不断增加。在《承诺确认书》及其章程的指导下，ICANN 在与 DNS 社群一起解决这些挑战方面承担着重大的责任。特别是，必须要建立全系统 DNS 应急计划、训练和协作响应功能。此概念文件为多利益主体讨论这些建议性新方案提供了依据，以便他们利用这些建议性新方案解决这些需求。