电信行业互联网网络安全监管现状与思考

付景广

信息产业部电信管理局

2007年4月

主要内容

- 我国公共互联网的基本情况
- 信息产业部互联网网络安全保障工作现状
- 关于加强互联网网络安全保障的若干思考

公共互联网的基本情况（1）

- 5家基础互联网运营企业（骨干+接入）
  - 电信、网通、移动、联通、铁通
  - 用户超过1.3亿，其中宽带用户超过7000万
  - 国际出入口带宽超过200G
  - CN顶级域名体系、根镜像服务器
- 互联网增值电信业务蓬勃发展
  - 信息服务业务（含网站、BBS、邮件服务、搜索服务、即时通信等，分为经营性、非经营性，需要许可或备案）
  - 接入和主机托管业务（ISP、IDC，需要许可）
  - 新业务（VoIP、P2P、IPTV等）

公共互联网的基本情况（2）

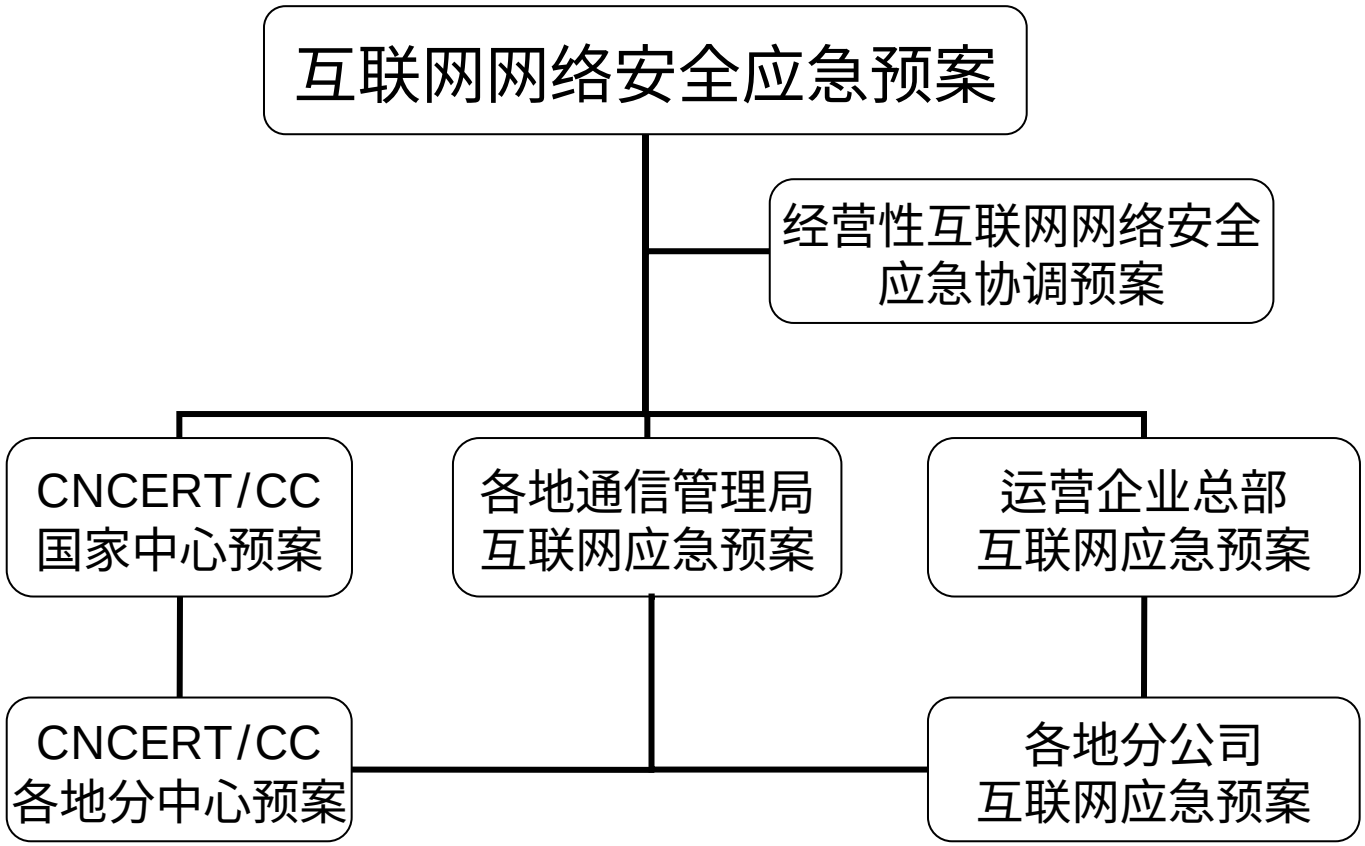
- 互联网网络安全问题日益突出
  - 网络病毒、网络攻击
  - 垃圾邮件、间谍软件、僵尸网络等
- 网络安全问题的危害日益严重
  - 对骨干网的可靠畅通构成威胁
  - 侵害应用服务提供者的利益
  - 侵害用户的切身利益
  - 影响人们使用互联网的信心，进而影响互联网发展

信息产业部互联网网络安全保障工作现状

- 网络安全应急体系建设
  - 事后的应急响应，努力减少事件造成的损失
- 网络安全防护体系建设
  - 事前的安全保护，努力减少事件的发生概率
- 网络信任体系建设
  - 网上身份认证和抗抵赖，努力打造诚信网络

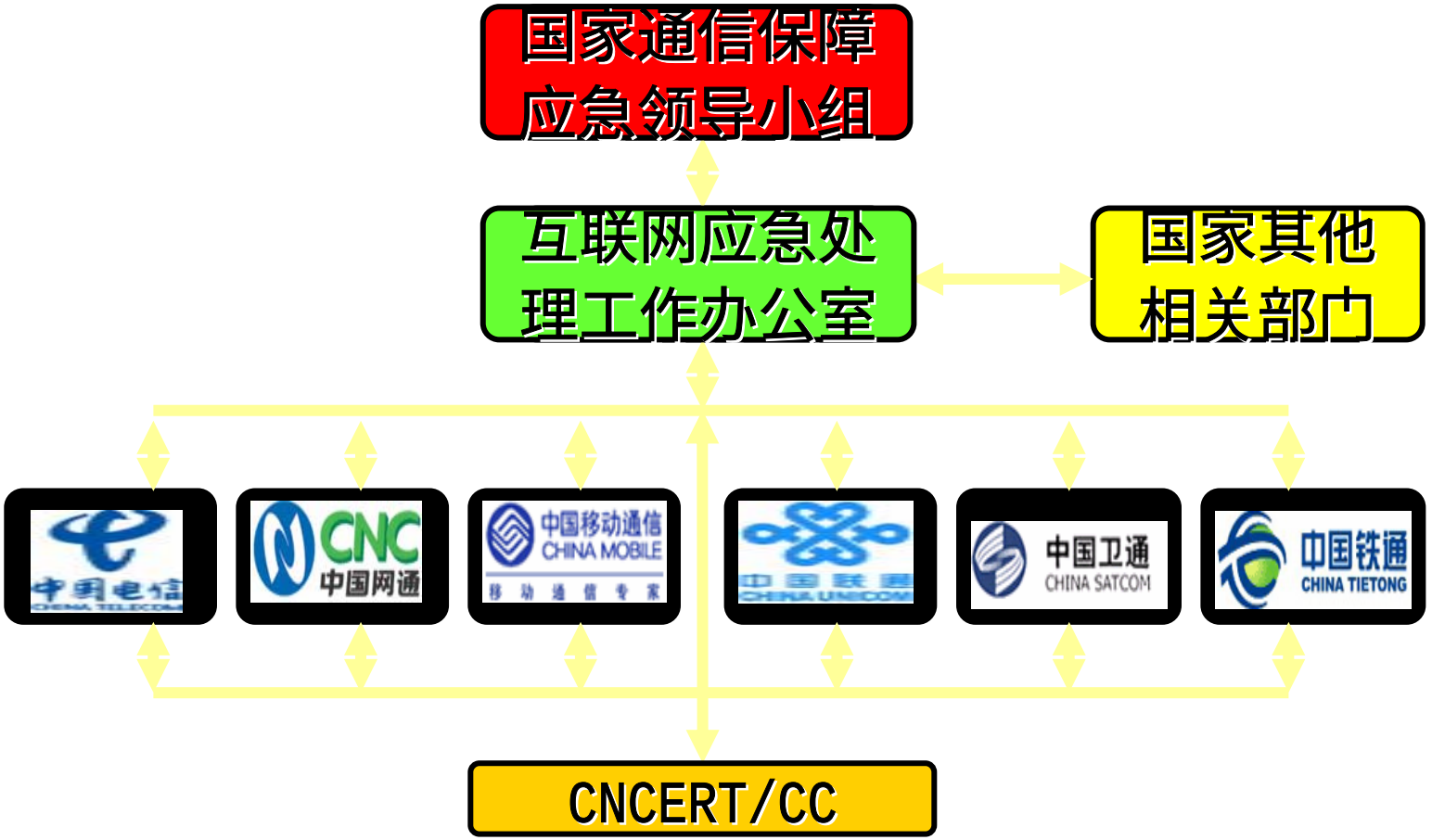
网络安全应急体系建设（1）

- 建立健全了公共互联网网络安全应急预案体系



网络安全应急体系建设（2）

- 加强了应急组织体系



网络安全应急体系建设（3）

- 应急工作中的主要机制
  - 监测/预警机制
  - 信息上报/通报机制
  - 常态下的定期联络会议机制
  - 对外协调机制（与非经营性互联网、公安部门等）

- 应急工作的主要特点
  - 只包括了基础运营企业
  - 主要针对比较严重的、大范围的网络安全事件，如：
    - 大面积断网
    - 骨干网络严重拥塞
    - 核心设备遭受攻击
  - 依靠专业的技术支撑队伍——CNCERT/CC

网络安全防护体系建设（1）

- 对基础互联网（骨干、接入部分）
  - 开展等级保护、风险评估和灾难备份工作
  - 制定安全防护措施要求（技术+管理）
  - 开展监督检查，进行安全评测和评估。

- 对互联网增值业务
  - 《增值电信业务网络信息安全保障基本要求》（YDN 126-2005）
  - 《防范互联网垃圾电子邮件技术要求》（YD/T 1311-2004）

网络安全防护体系建设（2）

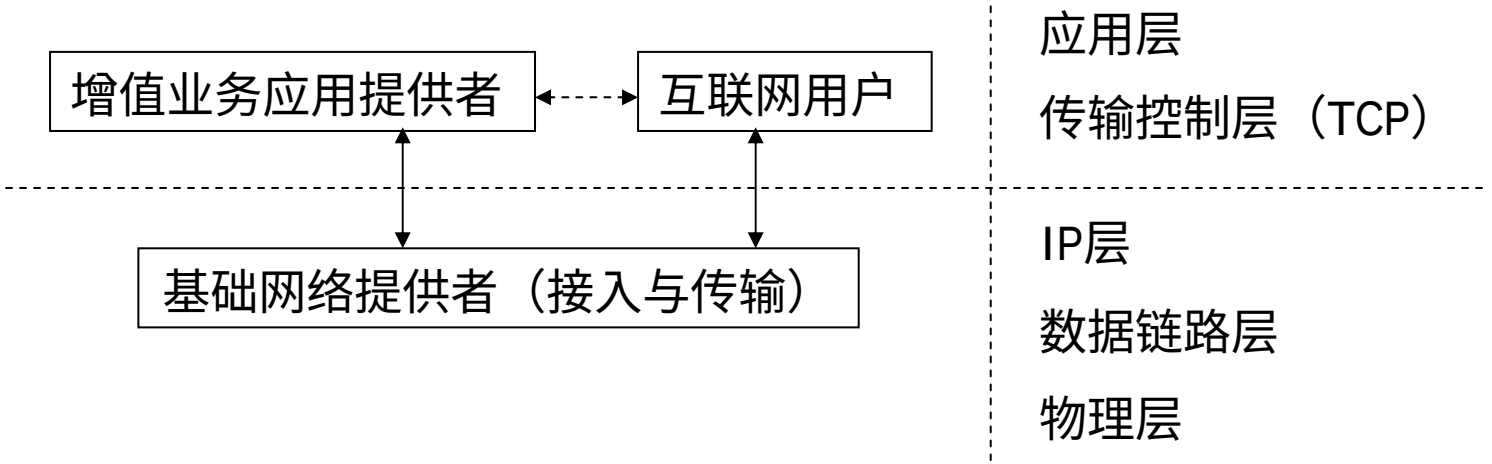
- 法律法规支持
  - 《电信条例》第五章“电信安全”部分
    - 关于规划、建设、运行“三同步”的要求
    - 关于不得危害网络安全的相关规定
    - 关于电信业务经营者应当加强内部安全保障的要求
  - 《互联网电子邮件服务管理办法》
    - 关于垃圾邮件相关行为的界定
    - 关于邮件服务提供者应当落实适当防范措施的规定
  - 《电信网络安全保障监督管理办法》（正在制订）
    - 关于基础网络等级保护、风险评估等制度要求
    - 基础运营企业的网络安全保障责任义务
    - 主管部门对保障工作的监督检查职责及流程

网络信任体系建设

- 按照《电子签名法》进行CA认证机构的规范管理
- 推广CA认证在电子政务、在线交易中的应用

关于加强网络安全保障的若干思考（1）

- 思考一：如何处理好底层网络安全、业务应用安全与用户安全之间的关系？



- 基础网络的基本安全需求：IP数据包端到端的可靠传输
- 业务应用的基本安全需求：业务应用系统的稳定运行
- 用户的基本安全需求：个人系统和数据的安全

关于加强网络安全保障的若干思考（2）

- 基础网络运营商可以为上层用户提供安全增值服务
  - 为增值应用服务商提供专业的安全保护和应急服务
  - 为普通用户提供在线的保护服务
  - 主观上是为用户，客观也提高了自身的安全性（比如可以减少流量异常事件）
- 增值应用服务商要为用户提供应用层的安全保障
  - 业务数据加密
  - 用户鉴别认证
  - 防止通过业务应用传播病毒、木马、垃圾邮件等
- 用户要提高网络安全意识和自我防范

关于加强网络安全保障的若干思考（3）

- 思考二：如何处理好电信行业与重要信息系统之间的关系？
  - 重要信息系统——金融、税务、海关、民航、铁路、电子政务等关系政治经济运行和国计民生的信息系统
  - 按照“谁主管、谁负责”原则，分别由各自主管部门负责保护和应急
  - 电信行业应提供高等级的支撑保障：
    - 保证日常传输线路的可靠畅通
    - 应急响应支持
      - 协调提供备用线路
      - 提供安全信息共享
      - 提供应急解决方案

关于加强网络安全保障的若干思考（4）

- 思考三：如何处理好网络安全保护、应急与打击网络违法犯罪之间的关系？
  - 区别：
    - 针对的对象不同：
      - 保护和应急针对的是网络的相关客体
      - 打击网络违法犯罪针对的是破坏网络安全的行为主体
    - 目的意义不同
      - 保护和应急是被动的防守和反应，重在“治标”
      - 打击网络违法犯罪重在“治本”
  - 联系：
    - 在保护和应急过程中要注意为打击网络违法犯罪保留证据
    - 加强行业与执法部门之间的信息共享

谢 谢！