



# 电子政务外网 的顶层设计及实施建议

邵国安  
高级工程师

## 目录

- 国家相关文件的要求
- 国家电子政务外网的顶层设计
- 相关建议



- 统筹发展电子政务。建立国家电子政务统筹协调机制，完善电子政务顶层设计和整体规划。统筹共建电子政务公共基础设施，加快推进国家电子政务内网建设和应用，支持党的执政能力现代化工程实施，推进国家电子政务内网综合支撑能力提升工程。**完善政务外网，支撑社会管理和公共服务应用。**

-- 《国务院关于印发“十三五”国家信息化规划的通知》（国发〔2016〕73号）

- 推进整合，加快部门内部信息系统整合共享。推动分散隔离的政务信息系统加快进行整合。整合后按要求分别接入国家电子政务内网或国家电子政务外网的数据共享交换平台。

-- 《国务院办公厅关于印发政务信息系统整合共享实施方案的通知》（国办发〔2017〕39号）

- 国家政务服务平台依托国家电子政务外网建设，主要实现各地区各部门政务服务汇聚、跨地区跨部门数据交换、跨地区统一认证、共性基础服务支撑。

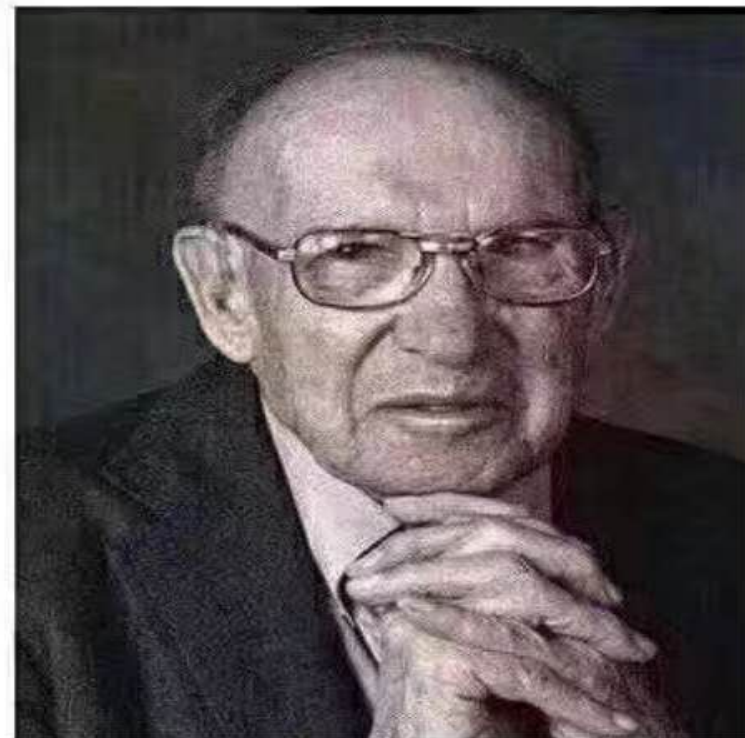
-- 《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办函〔2016〕108号）

- 顶层设计 Top-level design
- 自顶向下**规划**Top-down planning
- 自顶向下设计 Top down design
- 自底向上设计Bottom-up design
- **顶层**----自上而下的战略目标的**制定**（ 5~10年 ）
- **设计**----自下而上的计划预算、方案的**落实**（ 每年预算 ）
- 所谓**战略**：就是从全局考虑谋划实现整体目标的规划。

- **定位：**各级政务部门的非涉密业务专网，与互联网逻辑隔离
- **战略目标：**
  - 专线连接国家、省、地、县的各级政务部门及相关事业单位
  - 国家电子政务的关键基础设施
  - 承载社会管理、公共服务、业务协同、应急处置等政务业务
  - 实现数字政府的各项业务目标和政务目标
  - 引领国家信息化的深度发展，实现数字经济发展、振兴中华民族的伟大复兴

彼得·德鲁克(Peter F. Drucker ,  
1909.11.19~2005.11.11)

现代管理学之父，其著作影响了数代追求创新以及最佳管理实践的学者和企业家人，各类商业管理课程也都深受彼得·德鲁克思想的影响。



**战略不是研究我们未来要做什么  
而是研究我们今天做什么才有未来**

—— 德鲁克



# 问题

- 关口的定位是什么？内容包含哪些？
- 网络安全的关口前移，移到哪？
- 我们应该怎么做？从哪里做起？

# 全方位的网络安全保护要求

- **边界安全**

- 与互联网的连接（ISP）、与移动运营商的VPDN连接、各局域网出口与政务外网的连接及其他专线的边界
- 基于行为、攻击攻击、特征匹配、DNS监控、NAT及域名监控

- **安全防护**

- 各类安全防护设备的日志、安全策略及基于行为实时监测、网络流量的监测、网络行为审计

- **终端安全**

- 对各类PC终端的管理：操作系统、各类物联网前端、病毒补丁管理、DNS管理及访问控制

- **应用安全**

- 应用系统源代码管理、网络信任体系（身份认证、授权管理和责任认定）及系统补丁管理

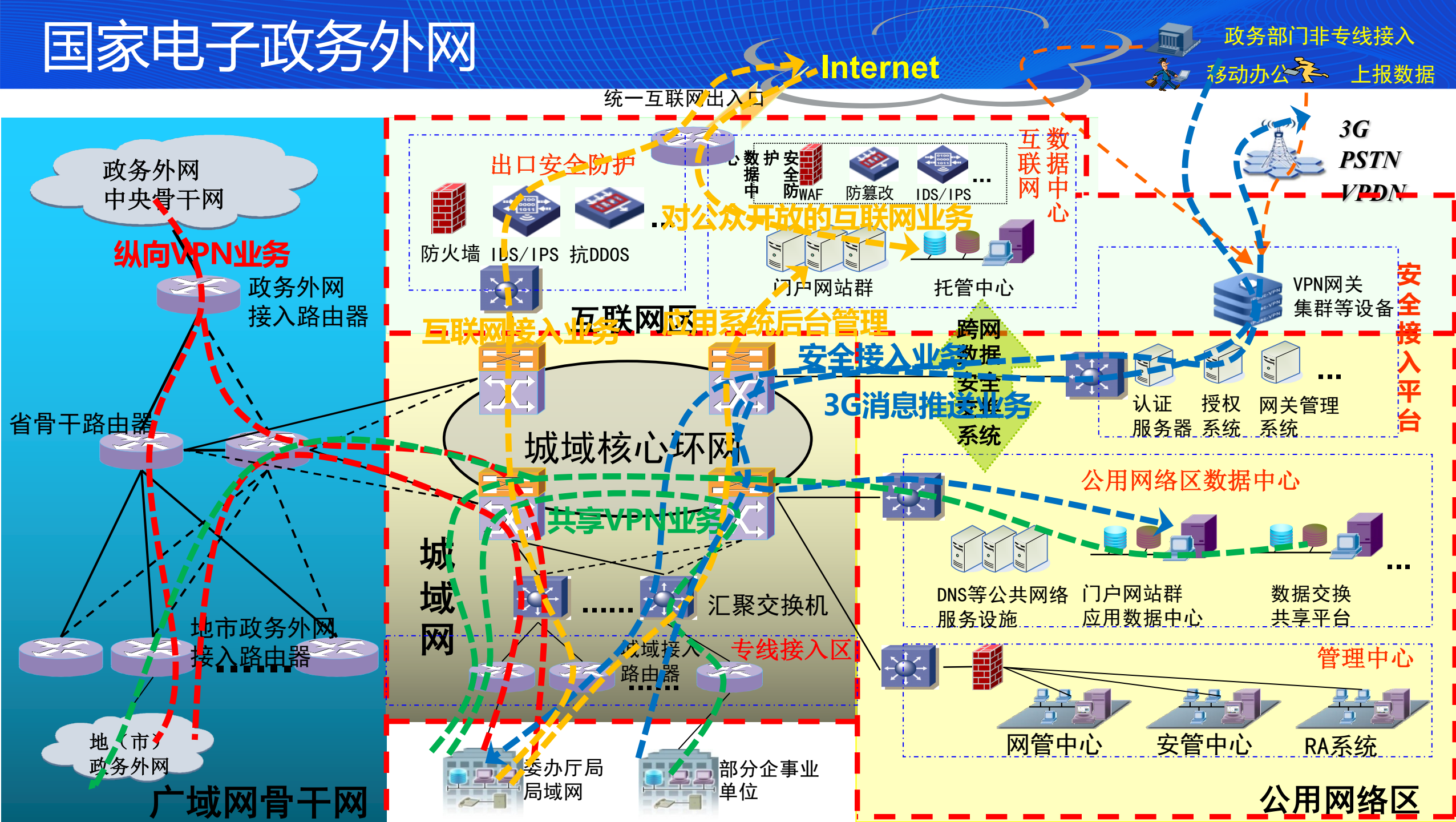
- **数据安全**

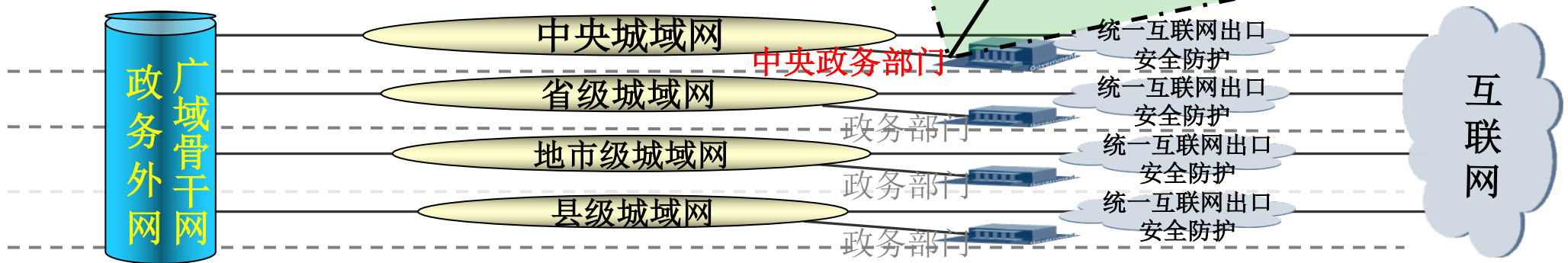
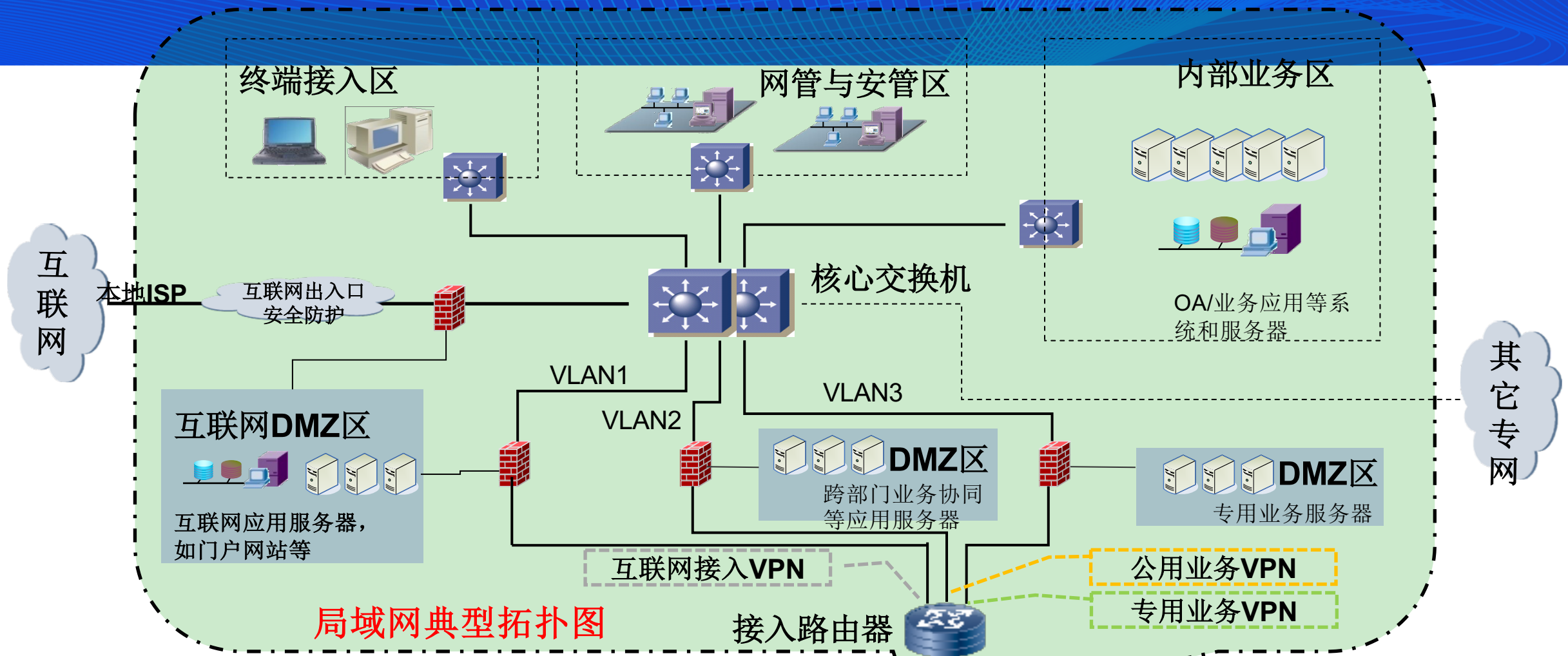
- 数据从产生、传输、使用、共享、存储、销毁，数据加密、数据库审计，作为资产进行管理

- **网络内容及舆情**的安全



# 国家电子政务外网

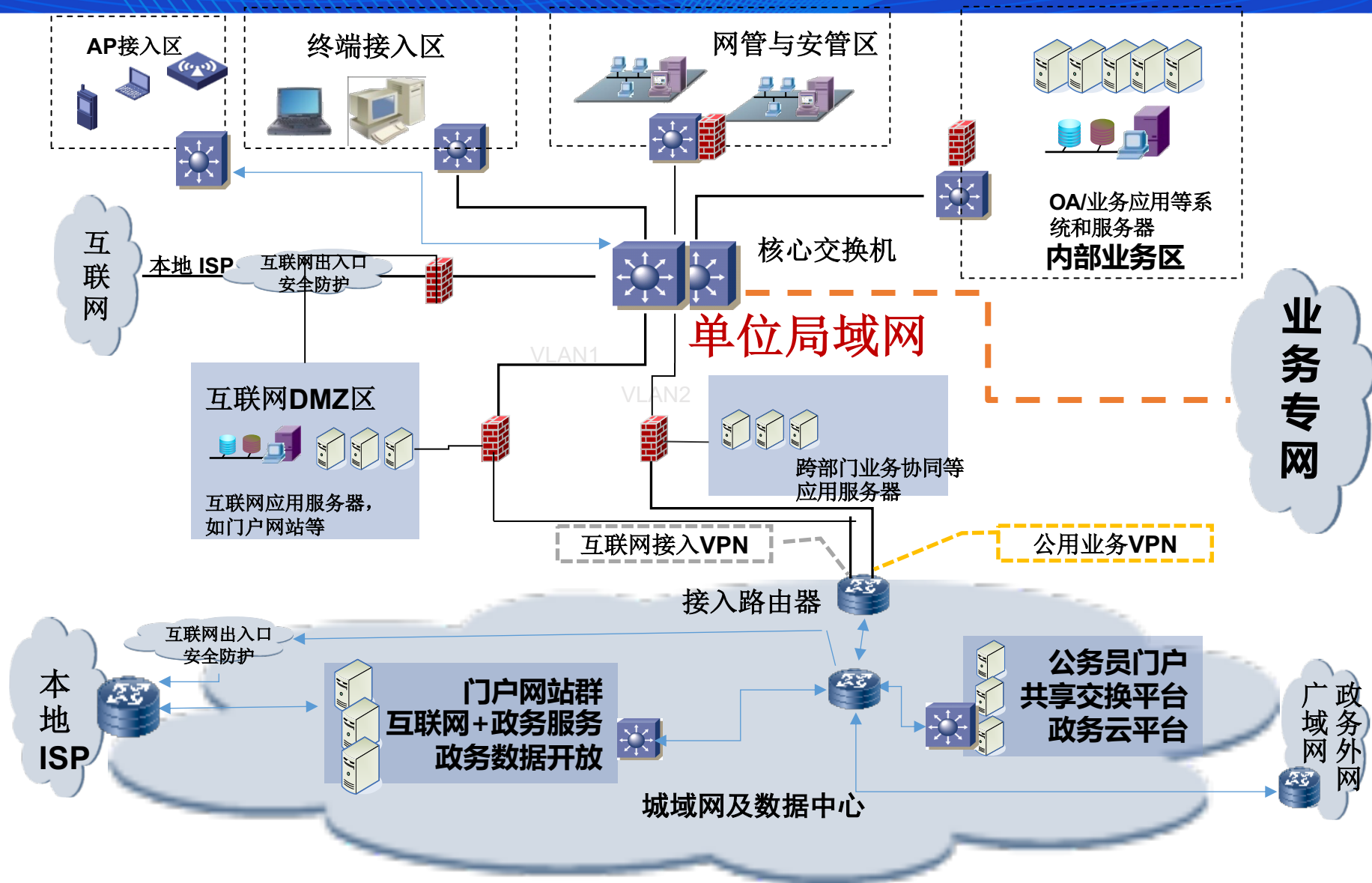




# 政务外网与业务专网的关系

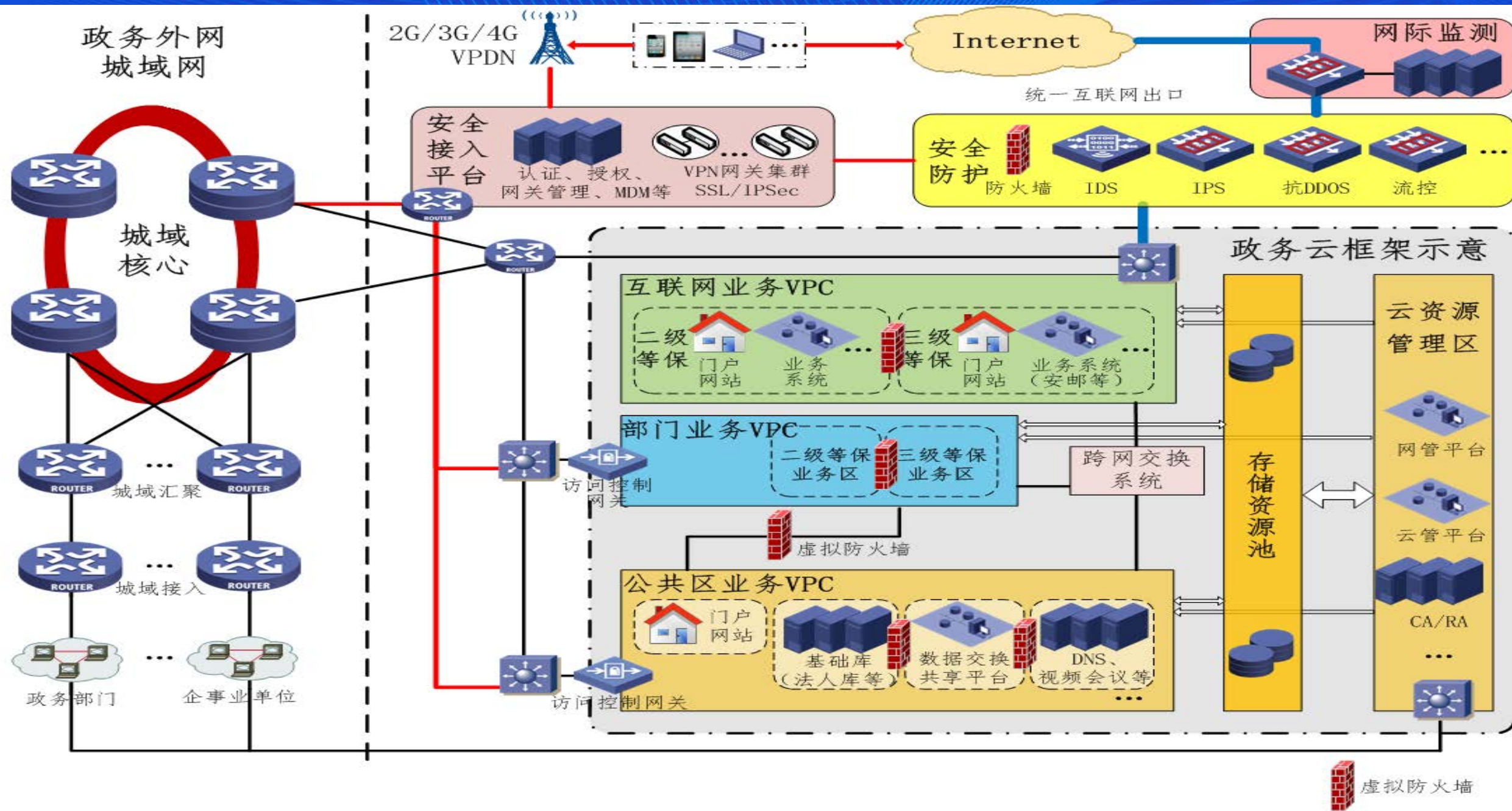


《信息化建设》  
2018年第11期，  
P20: “协同发展  
国家政务外网和  
业务专网”





# 政务云与政务外网、互联网的关系及要求



- 电子政务可分解为政务**内部**业务和**开放**业务
- **内部**业务可分为部门内部自身业务和跨部门共享与交换业务，如公务员门户或政务信息共享网站（[data.cegn.cn](http://data.cegn.cn)）
- **开放**业务部署在互联网上，又可分为信息公开类，如网站（[www.gov.cn](http://www.gov.cn)）、政务数据开放网站（[www.data.gov.cn](http://www.data.gov.cn)）及政务服务类（如网上预约、业务办理、项目申报等）

- 信息**公开**

- 通过新闻、媒体、广播、电视、电台、互联网等各种能够获取的各类信息，属于政府主动发布的信息

- 政务数据**开放**

- 经过数据加工、整合，能够被机器识别的可机读的数据，如CSV、XMIL格式
- 企业或用户申请才能得到
- 部署在政府专门的网站，如data.gov.cn

- 数据**共享与交换**

- 在网络可达的前提下实现，政务内部使用、跨部门、跨省使用，满足各部门的数据共享与交换、业务协同、应急处置等需求。

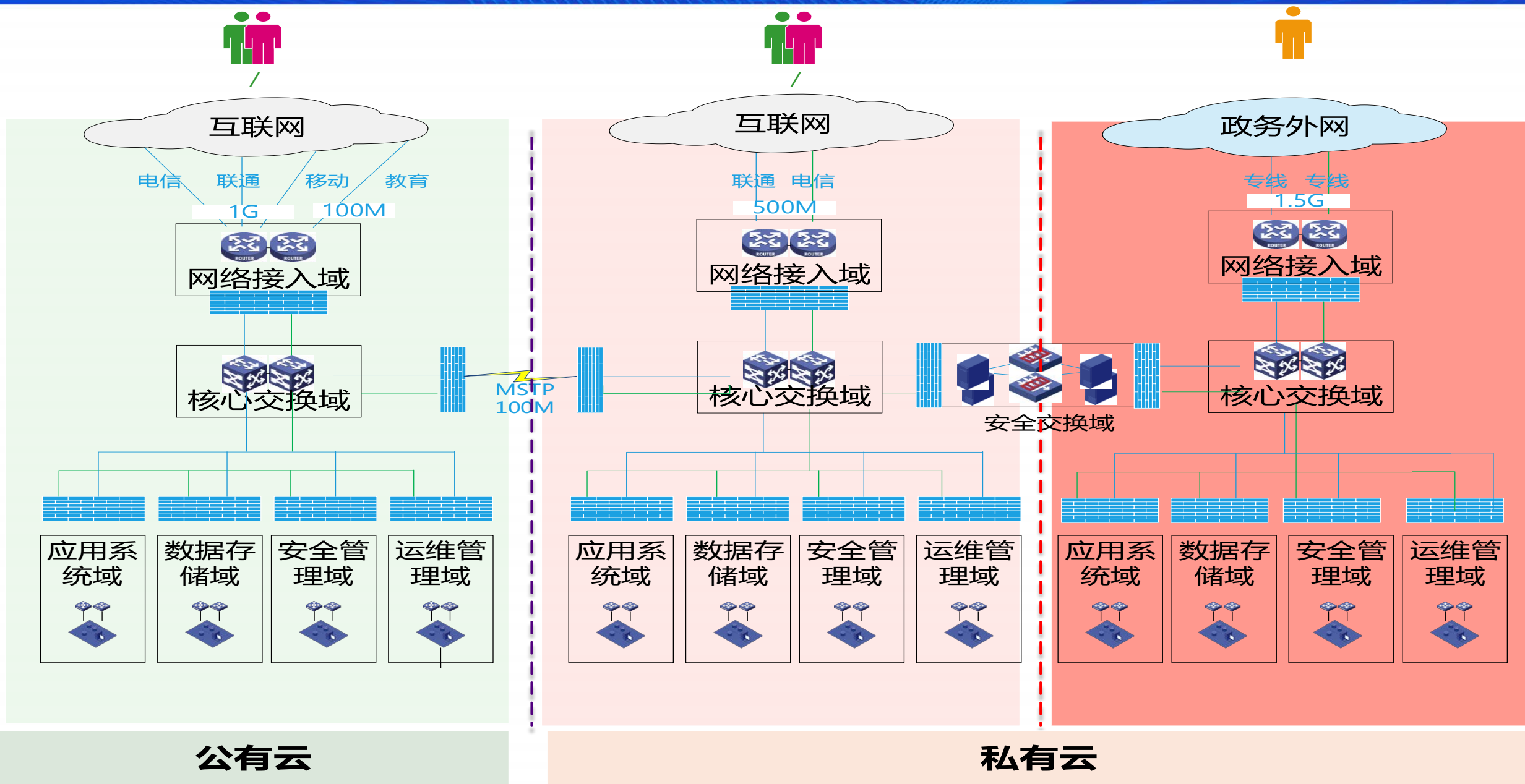


- 通过互联网为企业事业单位、公民提供更好、更方便的服务，以人为本，通过信息化手段，建立和谐社会和服务型政府
  - 政务数据**共享与交换**，实现跨部门、跨地方的业务协同、社会管理和公众服务
  - **开放**政务数据，释放企业活力、提高企业创新能力，引领社会和国民经济的发展
  - 充分**利用现有资源**，实现资源整合、业务融合、开放共享、提高服务水平和用户体验

( 国发[2018]27号 )

- 加快建设全国一体化在线政务服务平台，推进各地区各部门政务服务平台规范化、标准化、集约化建设和互联互通，形成全国政务服务“一张网”。
- 政务服务流程不断优化，全过程留痕、全流程监管，政务服务数据资源有效汇聚、充分共享，大数据服务能力显著增强。
- 政务服务线上线下融合互通，跨地区、跨部门、跨层级协同办理，全城通办、就近能办、异地可办，服务效能大幅提升，全面实现全国“一网通办”，为持续推进“放管服”改革、推动政府治理现代化提供强有力支撑。
- 全国一体化在线政务服务平台由国家政务服务平台、国务院有关部门政务服务平台（业务办理系统）和各地区政务服务平台组成。

# 国家政务服务平台总体技术架构





# 国家政务服务平台总体框架

用户



自然人/法人/其他  
社会组织



政务服务平台工  
作人员

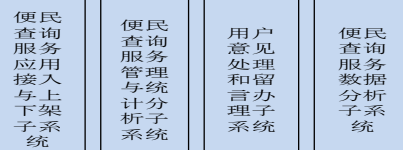


管理人员

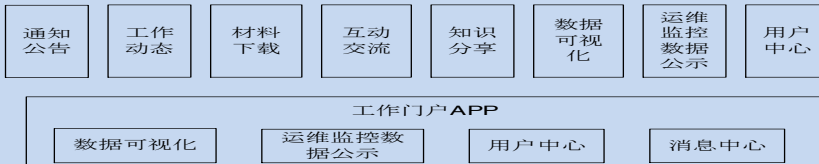
服务门户



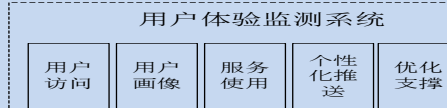
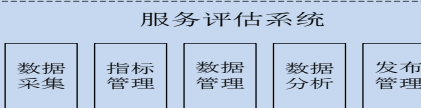
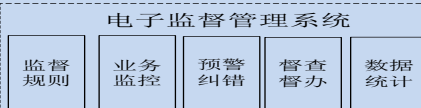
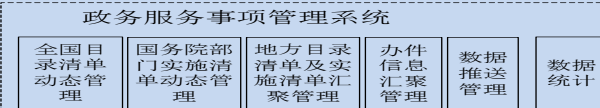
中国政府网、国务院客  
户端衔接与改造



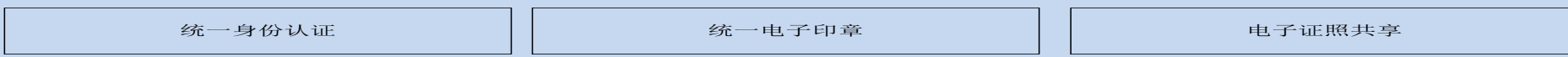
国家网上政务服务工作门户



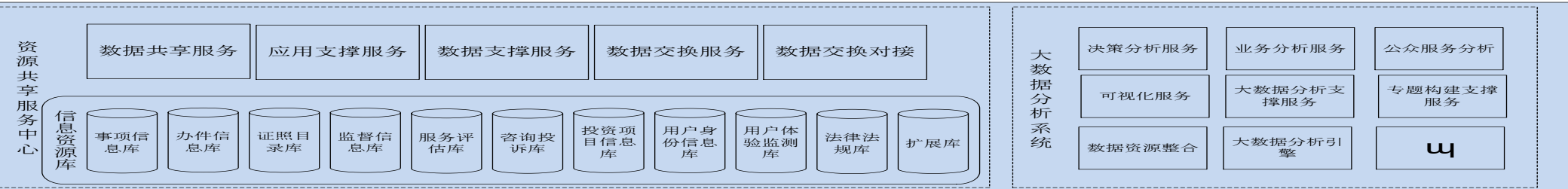
业务应用层



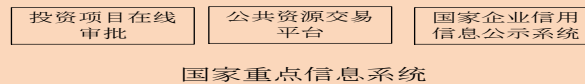
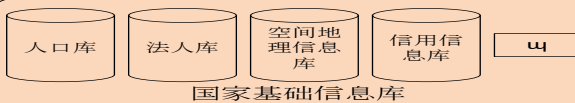
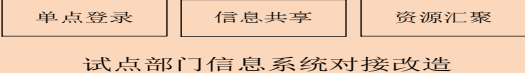
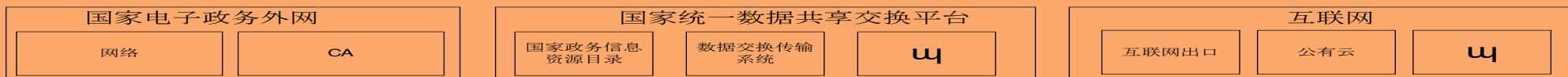
公共支撑层



数据资源层



基础设施层



相关外部信息系统

安全和运维保障体系

# 国家政务服务平台功能模型设计

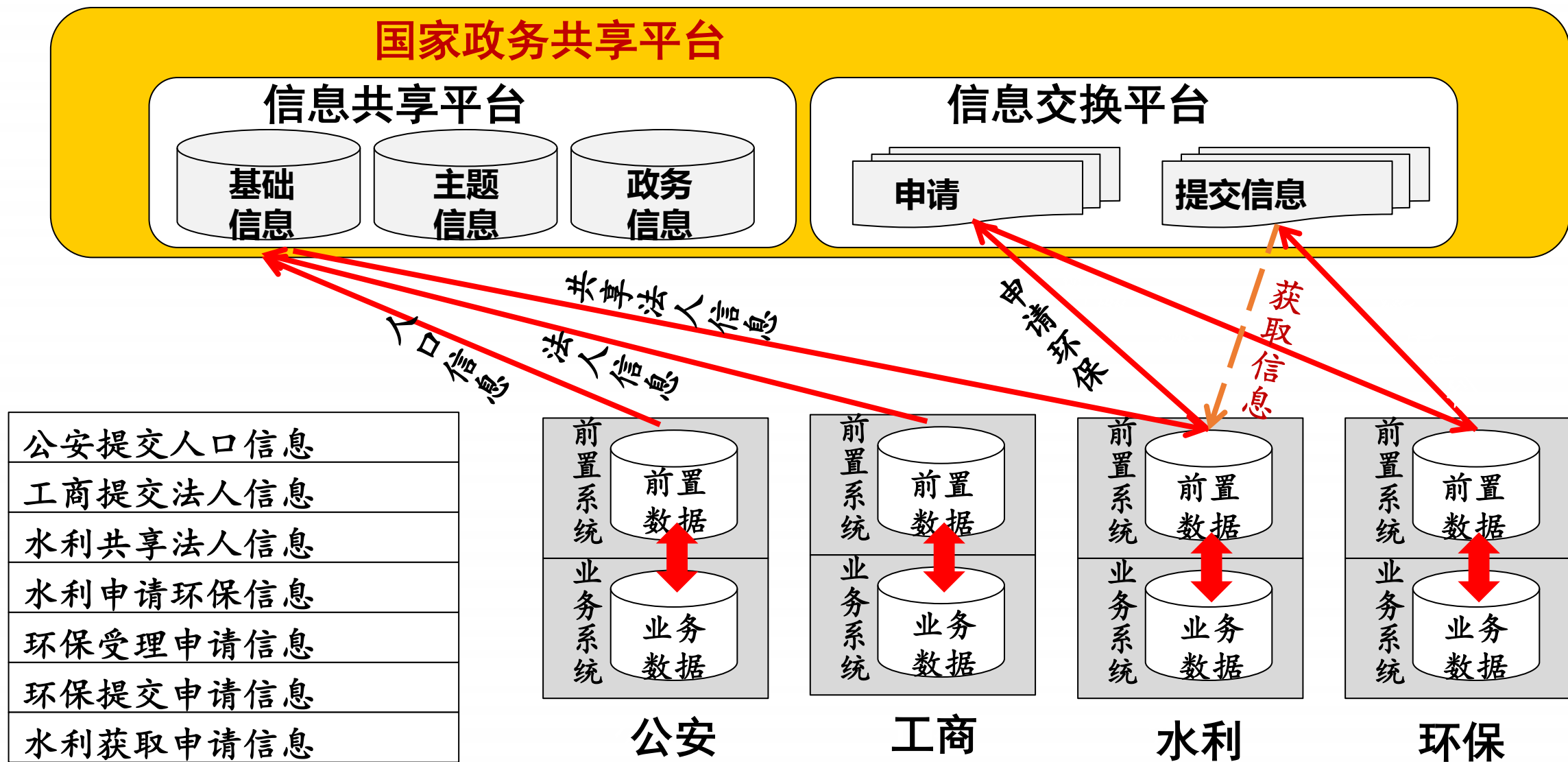


## 一体化在线政务服务：

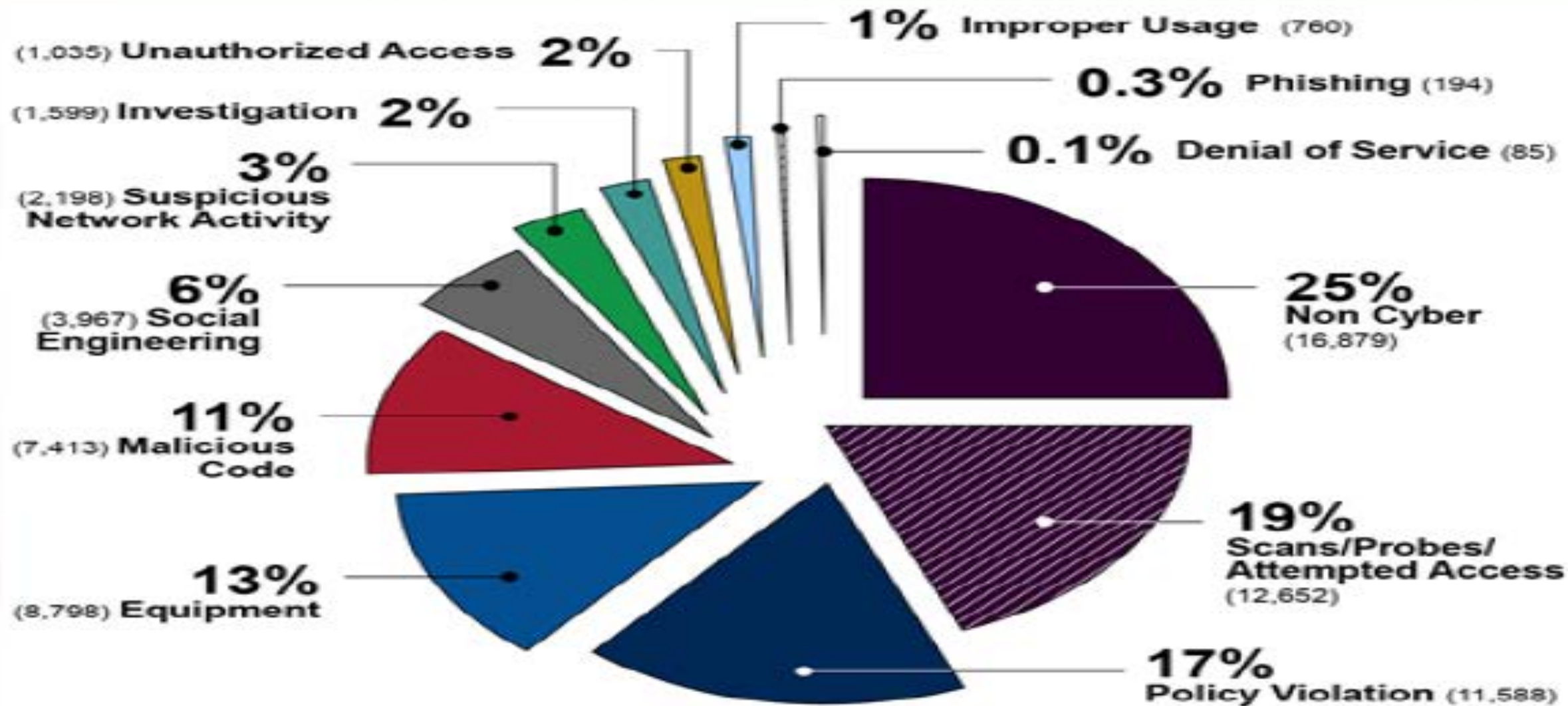
- **一体化**指国家、省、地、县各级政务部门的业务协同和联动。其关键技术是跨部门跨省的数据共享与交换
- **在线**指法人和自然人在互联网上可以24小时提交相关材料。其关键技术是互联网+可信身份认证



# 信息共享基本原理——部门共享



网络安全事件报告的分级分类规范		
类别	一级分类	二级分类
0	授权训练、演习、调查	授权的渗透测试、漏洞扫描、安全检查等
1	成功入侵	木马入侵、病毒入侵、后门入侵、漏洞入侵、猜口令成功、网络攻击等
2	不成功的入侵行为企图	猜口令、SQL注入尝试等
3	拒绝服务攻击	短包、流量、DNS放大攻击等
4	违规行为	非法外联、安全策略不正确、误操作等人为事件
5	嗅探踩点	非授权漏洞扫描、常用服务探测等
6	可识别的异常	跨境数据传输、软件后门（尚未受控）、系统漏洞、不当使用、信息破坏、设备设施故障、灾害性事件等
7	其他未知异常	0day、通过行为分析的各类异常情况



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-714



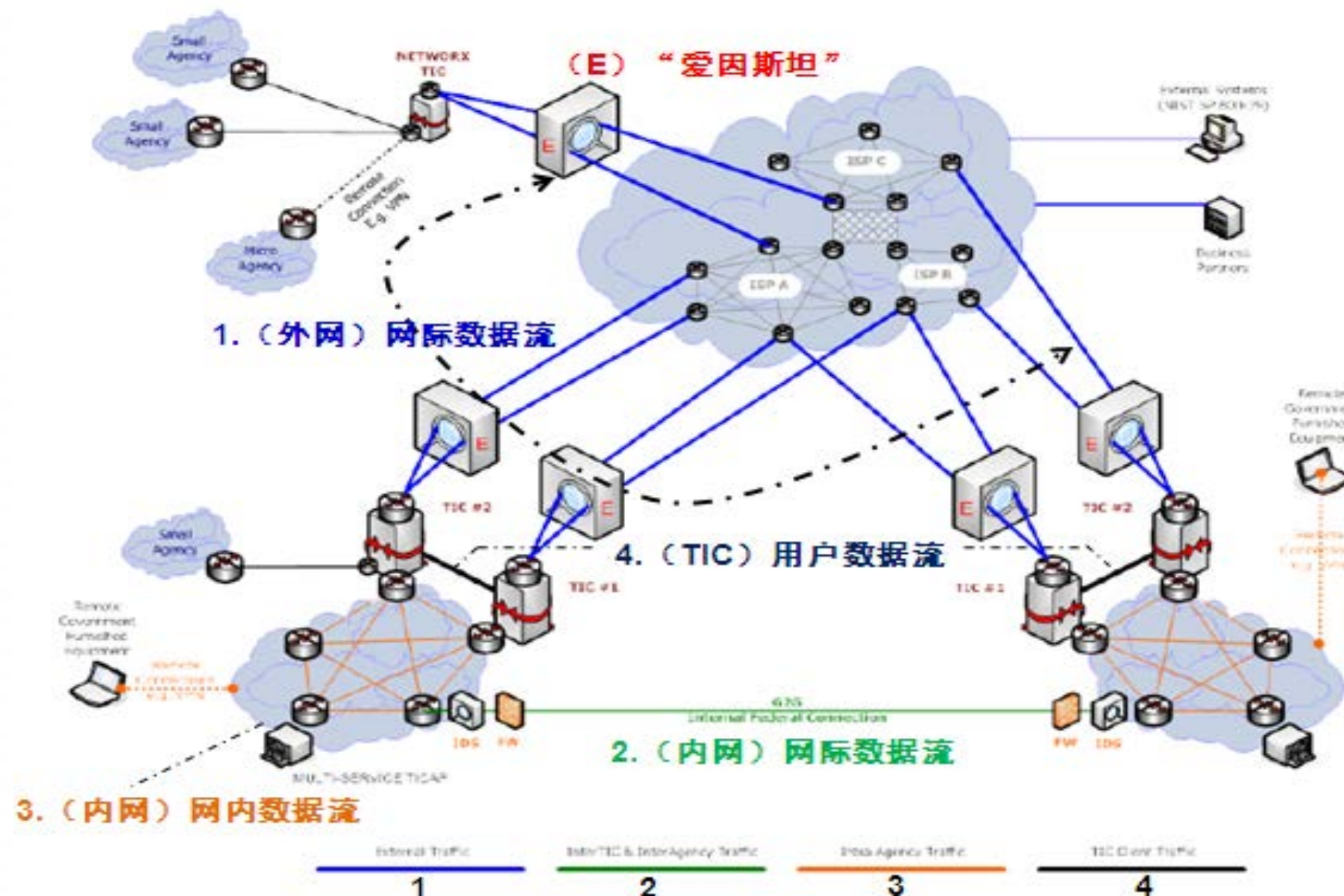
# 美国“爱因斯坦-3”（E3A）的应用定位

网络边界安全  
(Perimeter Security)

或  
网际安全

E3A串联在  
专用互联网与  
公共互联网之间

与可信互联网连接  
(TIC) 融为一体



# 网络边际及安全的定义

- **网络边际**(Network Perimeter)，明确为局部或专用网络与公共网络之间的**结合部**。

-----美国网络深度防御(Defense in Depth)

- **网际安全**（Cybersecurity）：是网络空间的一种属性，是抵抗有意和无意威胁，并对这些威胁作出响应和进行恢复的一种能力。

----- ISO/IEC 27032:2012, “Information Technology – Security Techniques – Guidelines for Cybersecurity”

明确**界定**网络安全的概念和**定义**，形成一致的**认知**框架，是做好一切网络安全工作的基础。

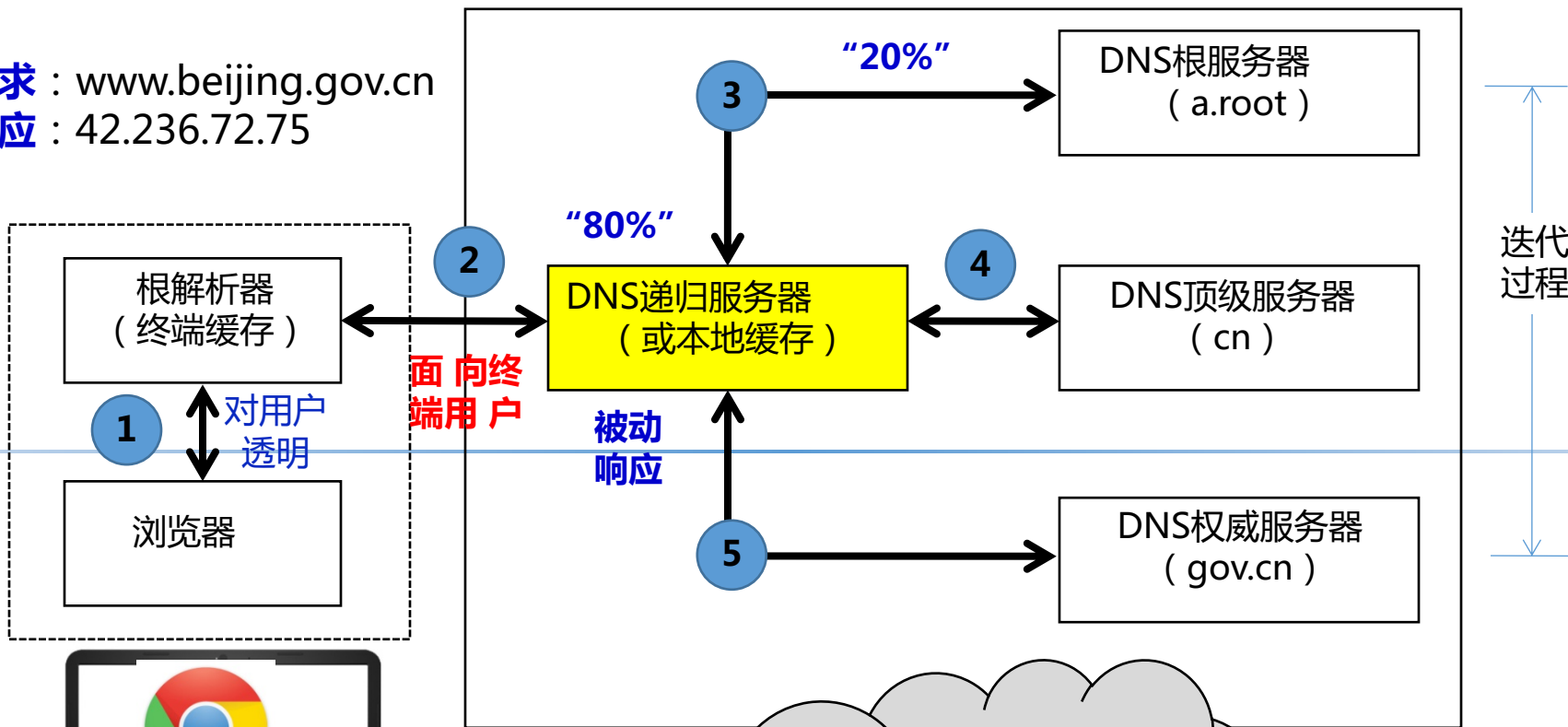
# 规范规则：DNS应用及服务的基本流程和过程

所有访问互联网均需要通过DNS，而DNS由递归DNS和权威DNS组成。

而权威DNS由根、顶级及权威服务器组成。

所以DNS元数据是互联网本源。

请求：www.beijing.gov.cn  
响应：42.236.72.75

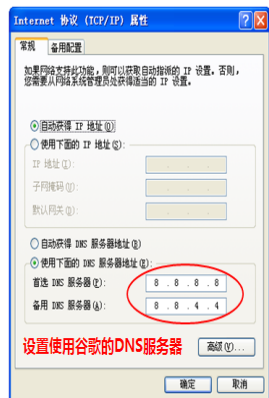


政务信息  
www.beijing.gov.cn

IP网络  
(公共互联网)

**“80/20规则”**

80%的DNS应用交互是在终端用户与DNS递归服务器之间；20%的DNS应用交互是在递归与迭代之间。



图例：

请求/响应的流程顺序



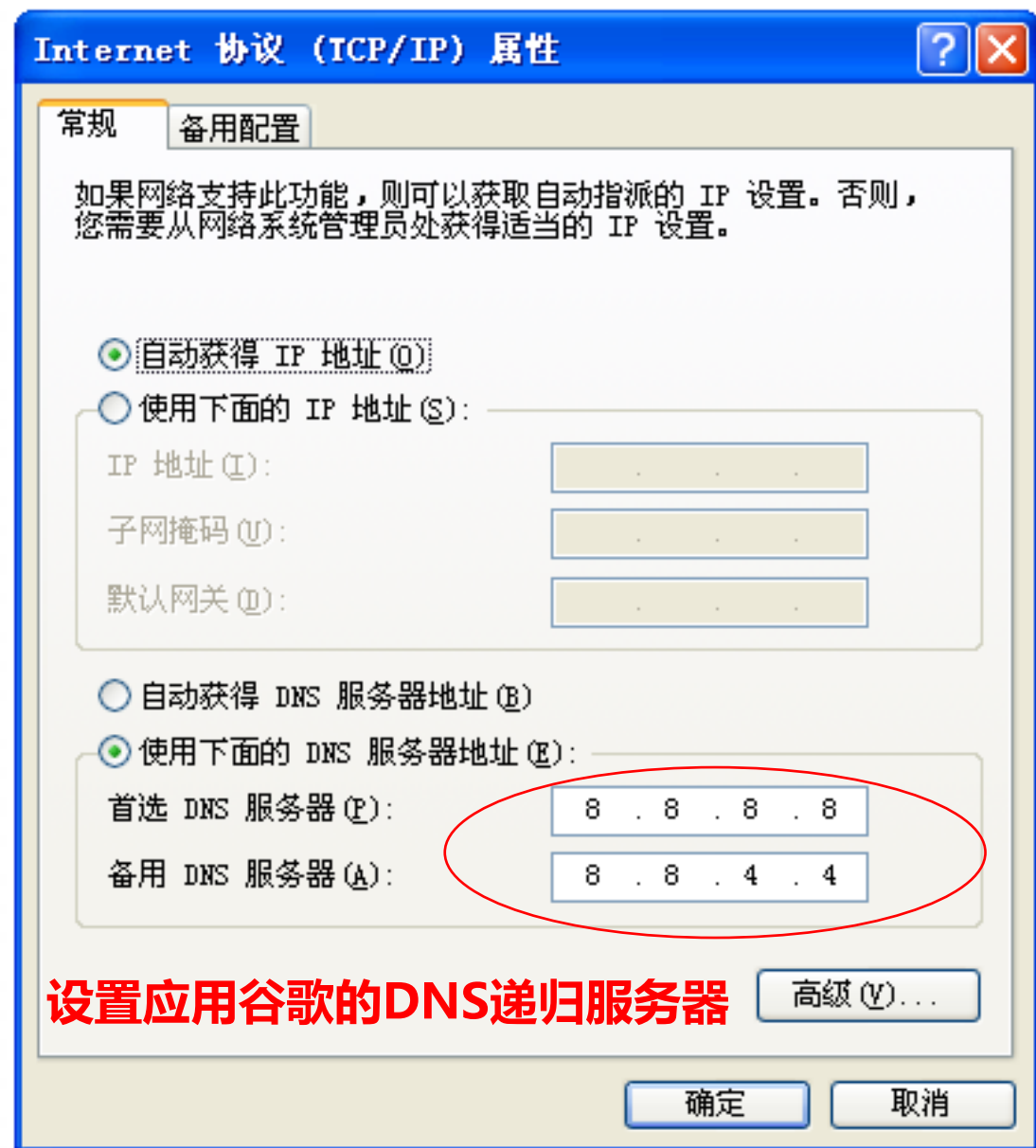
# 终端用户设置DNS应用的基本方式

在所有的用户和主机终端都必须配置DNS服务器

配置的方式包括：

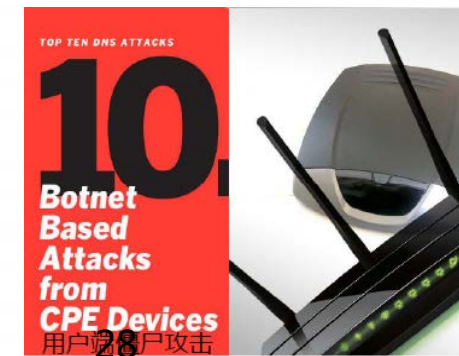
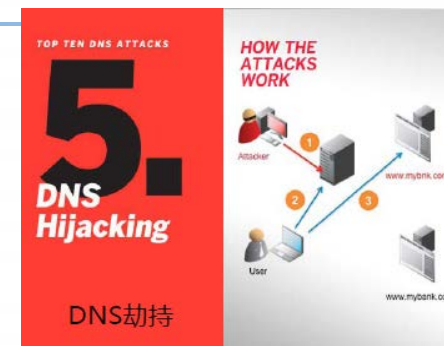
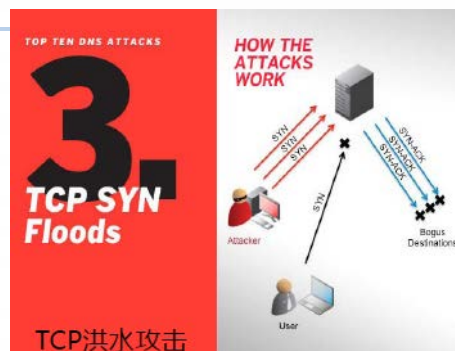
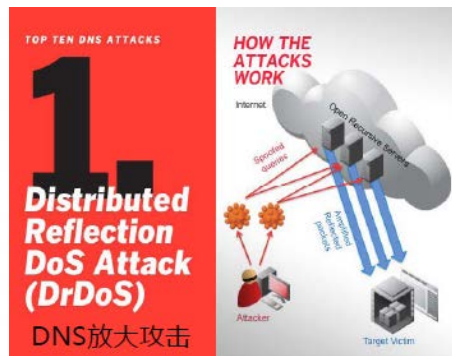
1. 系统管理员配置；
2. 系统自动获取；
3. 用户随意设置；
4. 恶意软件劫持；
5. 流氓软件绑架；
6. App软件篡改。

- 大多数终端用户默认（**对用户透明**）“系统自动获取”模式，这也给恶意、流氓、APP留下机会；
- “用户自行设置”模式造成滥用和误用，成为潜在的安全风险和隐患。



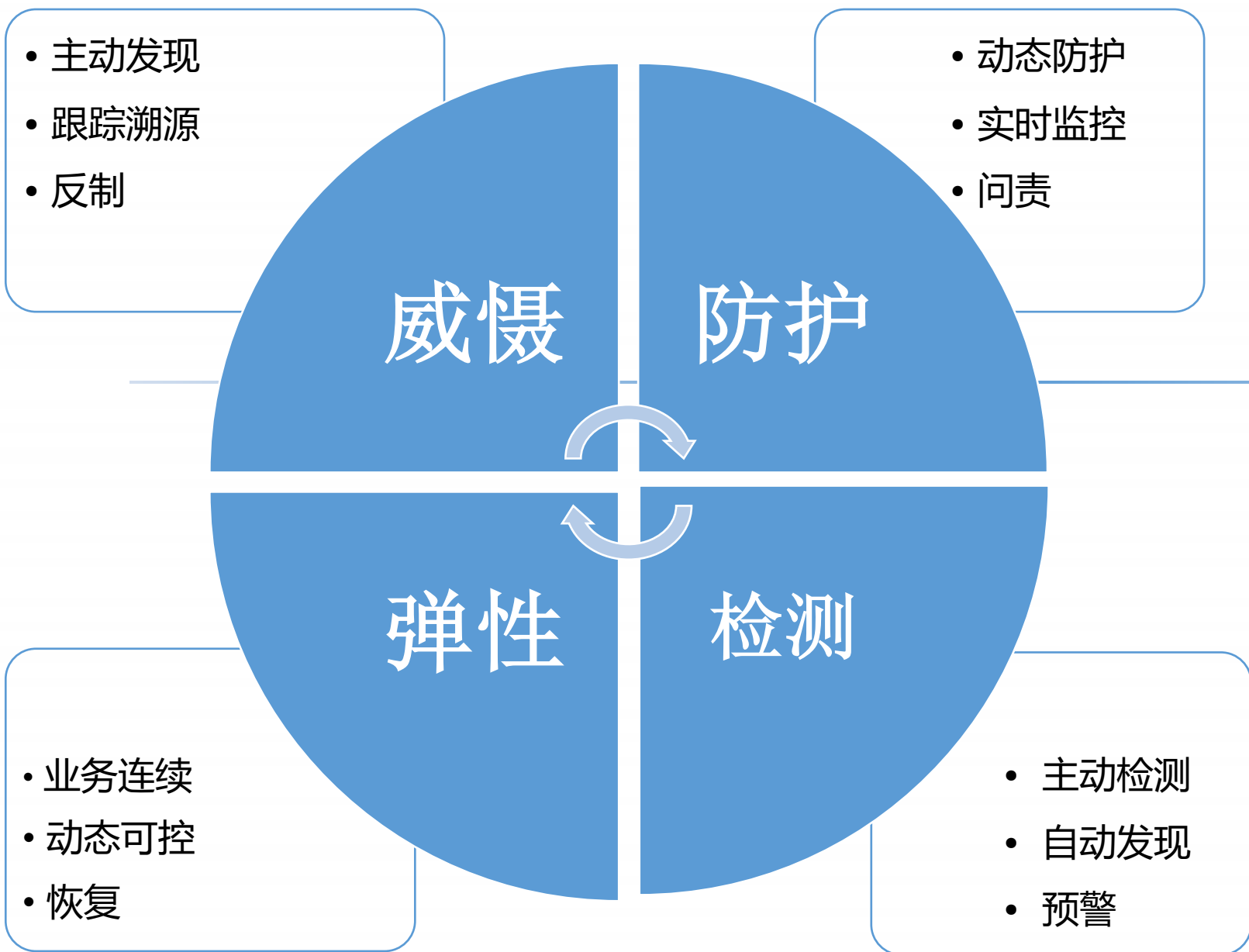
# 十种已知主要的DNS入侵模式和攻击方式

来源：《网络世界》  
( Network World )





# 具备主动免疫网络安全的主要特征






# 对首席信息安全官（CISO）的建议

- 网络安全的形势越来越复杂，国家的要求也越来越高，各单位对信息化安全的重要性的紧迫性认识也在提高，对安全公司CISO的建议：
  - ✓ 网络安全更多的是一种责任，需要高度自觉的责任感和使命感
  - ✓ 少跟风、少炒作，脚踏实地地研究产品和服务
  - ✓ 从网络安全对抗的本质来考虑产品和服务，为用户创造安全价值
  - ✓ 从全面的安全观来整体为用户制定网络安全战略
  - ✓ 认真学习美国等先进国家在网络安全上的做法、服务和产品

# 智慧源于对术语的定义

——苏格拉底



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

**2019北京网络安全大会**

2019 BEIJING CYBER SECURITY CONFERENCE