国家信息中心
State Information Center

国家电子政务外网管理中心
National E-Gov Network Administration Center

国家电子政务外网
安全保障及新技术安全问题的思考

外网办安全管理处　邵国安

2014年10月23日

地址：北京市西城区三里河路58号　邮编：100045　电话：010-68527618 68557203　传真：010-68533919

目 录

1 •国家电子政务外网应用情况及安全保障

2 • 新技术的应用给政务外网带来的安全挑战

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

国家信息中心
State Information Center

1

外网应用情况、安全保障

国家电子政务外网应用情况及安全保障

地址：北京市西城区三里河路58号　邮编：100045　电话：010-68527618 68557203　传真：010-68533919

国家信息中心
State Information Center

国家文件及政策规范要求（1）

- 《国家信息化领导小组关于我国电子政务建设指导意见》（中办发[2002]17号）
  - 政务外网与互联网之间逻辑隔离
  - 政务外网是政务的业务专网，主要运行政务部门面向社会的专业性服务业务和不需在内网上运行的业务

- 《国家信息化领导小组关于推进国家电子政务网络建设的意见》（中办发[2006]18号）
  - 政务外网主要满足各级政务部门社会管理、公共服务等面向社会服务的需要
  - 政务内网和政务外网的建设要按照信息安全分级保护和等级保护的有关要求，分别采取相应的保护措施。

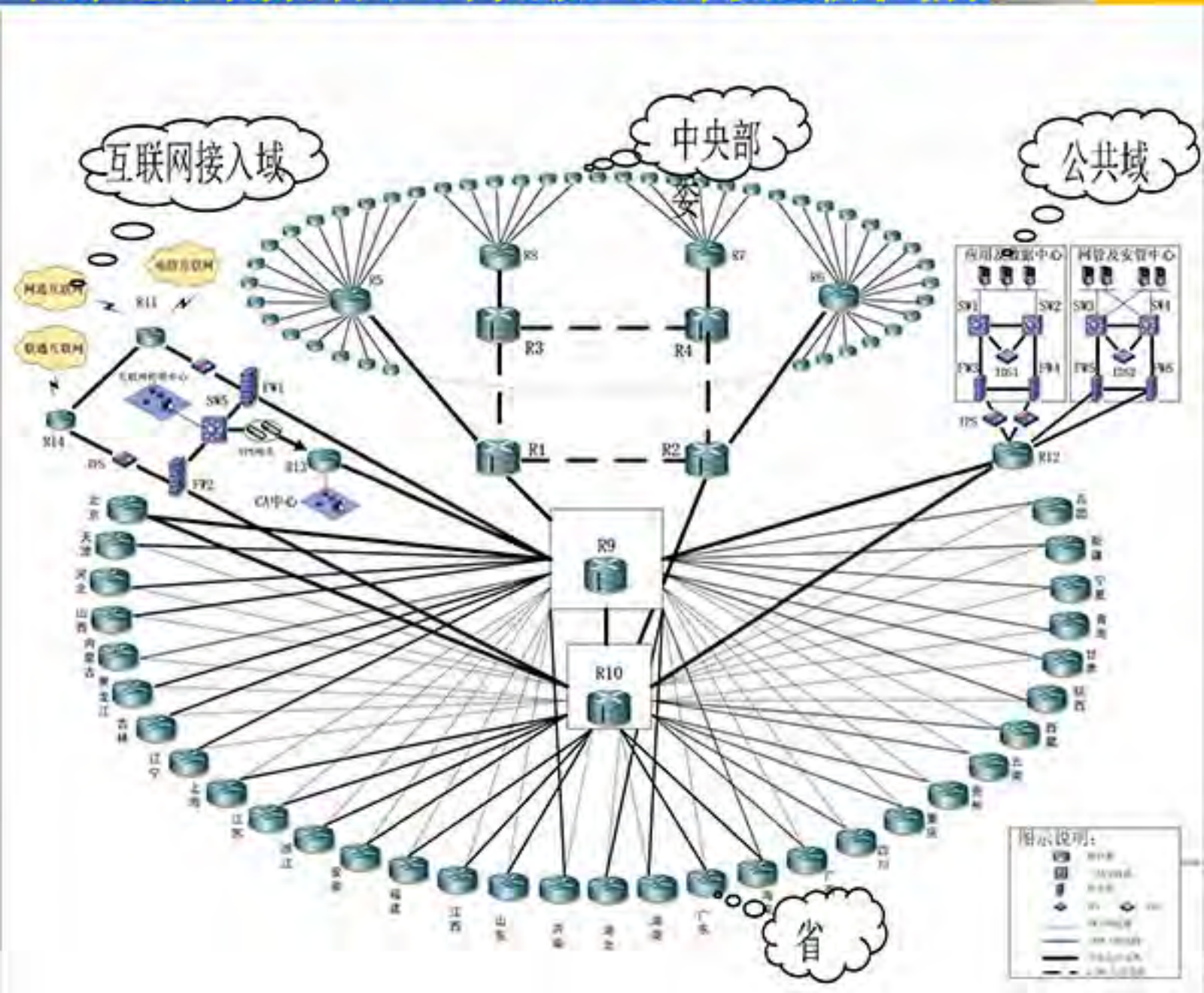
国家文件及政策规范要求（2）

- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
  - 信息安全保障工作是坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。
  - 信息安全监控是及时发现和处置网络攻击，防止有害信息传播，对网络和系统实施保护的重要手段
  - 建立健全指挥调度机制和信息安全通报制度
  - 信息安全建设是信息化的有机组成部分，必须与信息化同步规划、同步建设
  - 建立和落实信息安全管理责任制。谁主管谁负责、谁运营谁负责

国家文件及政策规范要求（3）

- 国函[2012]36号
  - 完善国家电子政务外网，整合地方网络资源，加大地方政务外网的建设，推进中央与地方各级政务外网的联通。
  - 各项目建设必须充分利用统一的国家电子政务网络，避免重复投资、重复建设。
- 发改高技[2012]1986号
  - 建设完善国家电子政务网络体系
  - 各政务部门新建和续建电子政务项目，应纳入国家电子政务网络体系，部门专网业务向电子政务网络体系的迁移。

国家电子政务外网（中央级）基本安全防护情况




已有21省市区+新疆兵团覆盖到县
海南已覆盖除三沙市外各市县
6省区正在向县级延伸

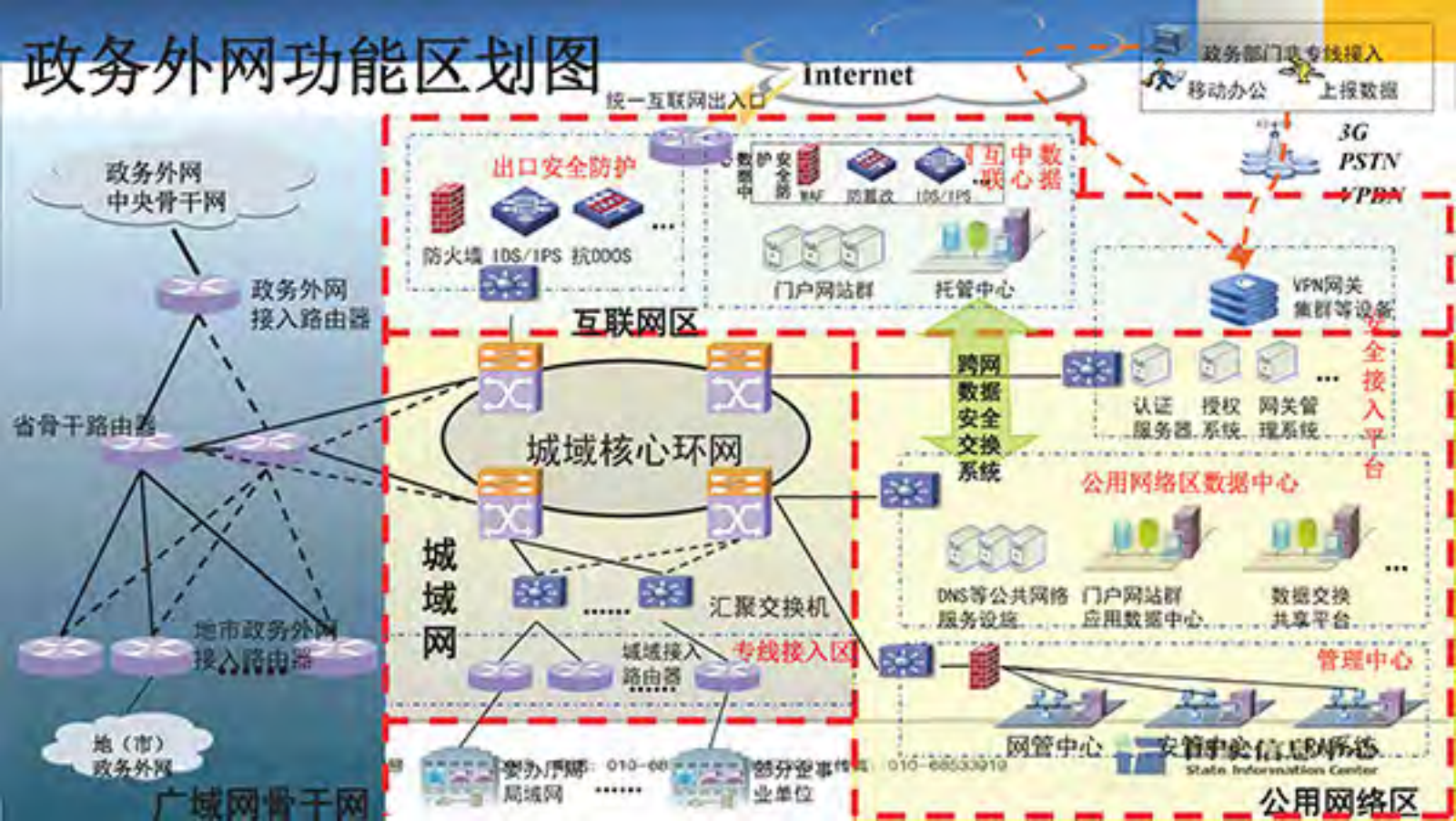

应用支撑服务
信息资源目录
数据交换平台
大文件传输
门户网站
数据中心服务
设备托管
数据存储
共享灾备
负载均衡
电子认证功能
数字证书
身份认证
电子签章
密钥管理
安全保障功能
安全防护服务
安全事件管理
安全检测
漏洞扫描
网络接入功能
专线接入服务
互联网
安全接入
互联网
出口服务
IP地址及
域名服务
全网统一标准规范和运行服务体系

中央政务部门利用政务外网开展的全国性业务

监察部—纠风系统
扶贫办—扶贫业务
文化部—文化共享工程
应急办—国家应急系统外网平台
农业部—金农工程
安监局—金安工程
国家知识产权局—专利电子审批系统
审计署—金审工程二期
新华社—新华频媒
出版署—新闻出版行业监管和服务信息系统
计生委—人口宏观管理与决策信息系统
总工会—全国工会系统工作动态等应用系统
中央纪委—查询全国组织代码电子档案
国家减灾中心—减灾救援项目
监察部—国家人口基础信息库先导工程

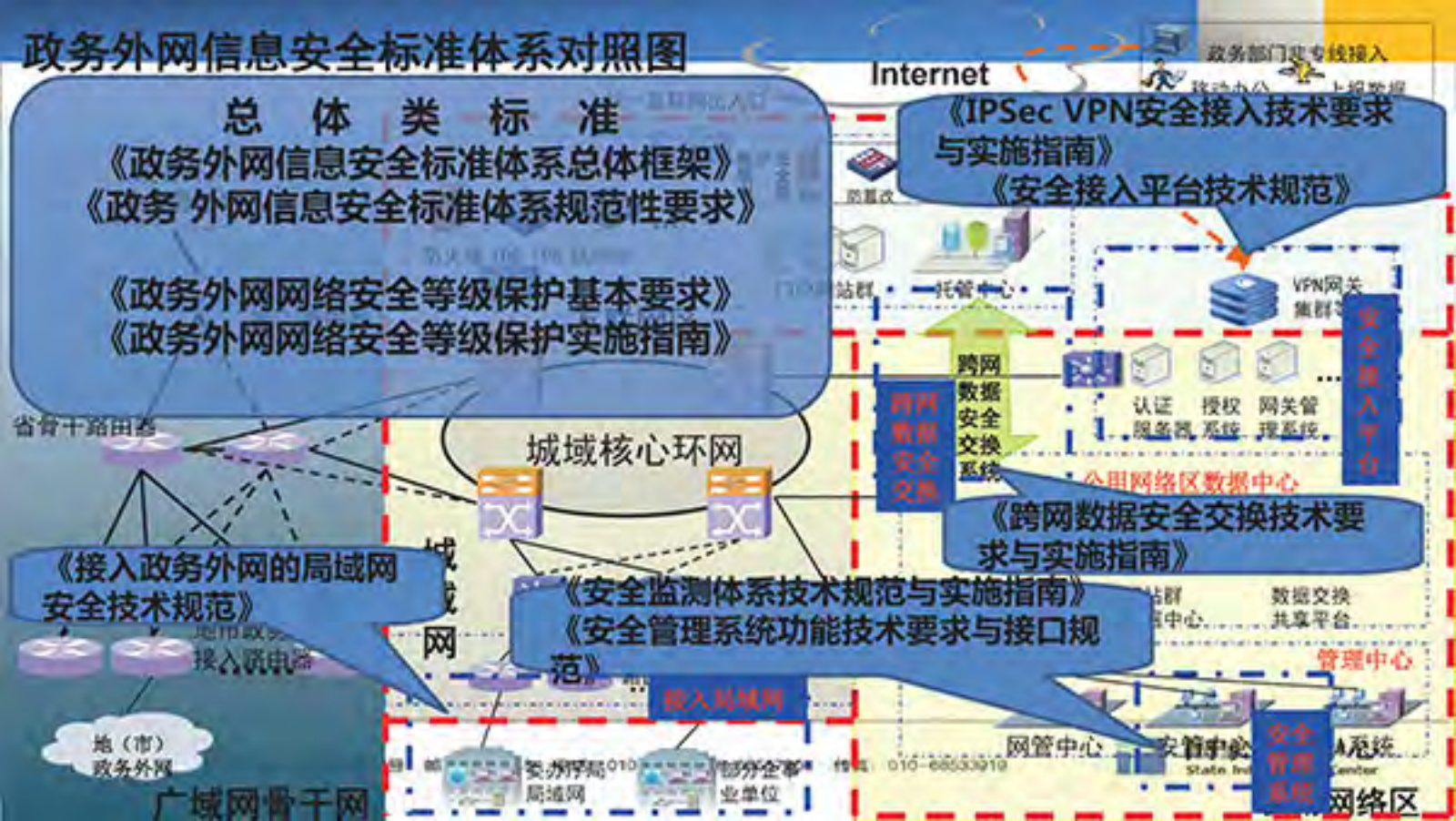
民建中央—中国民主建国会电子会务系统
质检局—金质工程
海关总署—海关专网备份网络
商务部—视频会议系统
科技部—全国科技信息服务系统
发改委—自然资源和空间地理基础库
环保部—国家环境信息与统计能力建设项目
人社部—国家公务员考试报名系统
卫生部—突发公共卫生事件应急指挥视频会议系统
交通部—海上联合搜救演习（一次性）
全国妇联—妇联信息化业务应用
国家民委—全国民族事务管理信息网络
中央综治办—全国社会管理综合信息系统
司法部—构建司法行政业务信息网络
国家密码管理局—密钥服务中心网络互联

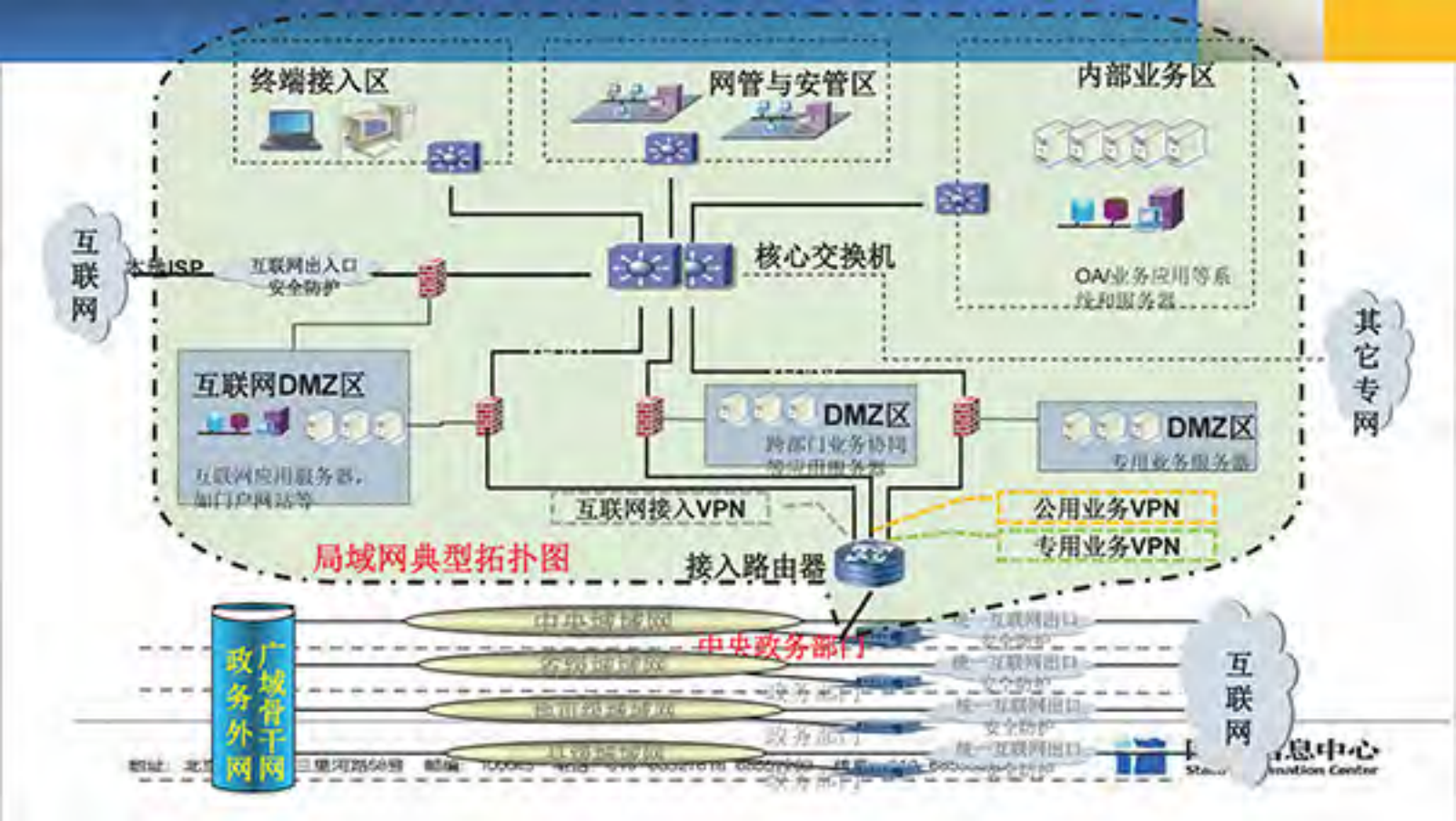
政务外网功能区划图


Internet
统一互联网出入口
政务部门业务专线接入
移动办公
上报数据
3G
PSTN
VPDN
政务外网
中央骨干网
政务外网
接入路由器
出口安全防护
防火墙 IDS/IPS 抗DDOS
互联网中心数据
防篡改 IDS/IPS
门户网站群
托管中心
互联网区
VPN网关
集群等设备
安全接入平台
跨网数据安全交换系统
认证服务器
授权系统
网关管理系统
省骨干路由器
城域核心环网
公用网络区数据中心
城域网
汇聚交换机
DNS等公共网络服务设施
门户网站群应用数据中心
数据交换共享平台
地市政务外网接入路由器
城域接入路由器
专线接入区
管理中心
网管中心
安全管理中心
State Information Center
地（市）政务外网
广域网骨干网
局域网
部分垂直业务单位
公用网络区


横纵向VPN与业务流向图
Internet
统一互联网出入口
政务部门专线接入
移动办公
上报数据
3G
PSTN
VPBN
政务外网
中央骨干网
纵向VPN业务
政务外网
接入路由器
出口安全防护
防火墙 IDS/IPS 抗DDOS
对公众开放的互联网业务
互联网中心数据
门户网站群
托管中心
互联网区
互联网接入业务
用户系统后台管理
安全接入业务
3G消息推送业务
数据交换系统
VPN网关
集群等设备
安全接入平台
认证服务器
授权系统
网关管理系统
省骨干路由器
城域核心环网
共享VPN业务
城域网
汇聚交换机
专线接入区
城域接入路由器
公用网络区数据中心
DNS等公共网络服务设施
门户网站群应用数据中心
数据交换共享平台
管理中心
网管中心
安管中心信息系统
State Information Center
地市政务外网接入路由器
地市政务外网
广域网骨干网
政务部门局域网
垂直业务单位
公用网络区

政务外网信息安全标准体系对照图




终端接入区
网管与安管区
内部业务区
互联网
核心交换机
互联网出入口
安全防护
互联网DMZ区
DMZ区
DMZ区
其它专网
互联网接入VPN
公用业务VPN
专用业务VPN
局域网典型拓扑图
接入路由器
中央政务部门
广域骨干网
政务外网
互联网

虚拟安全桌面解决方案

办公生产自由切换
终端数据存储隔离

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

国家信息中心
State Information Center

2

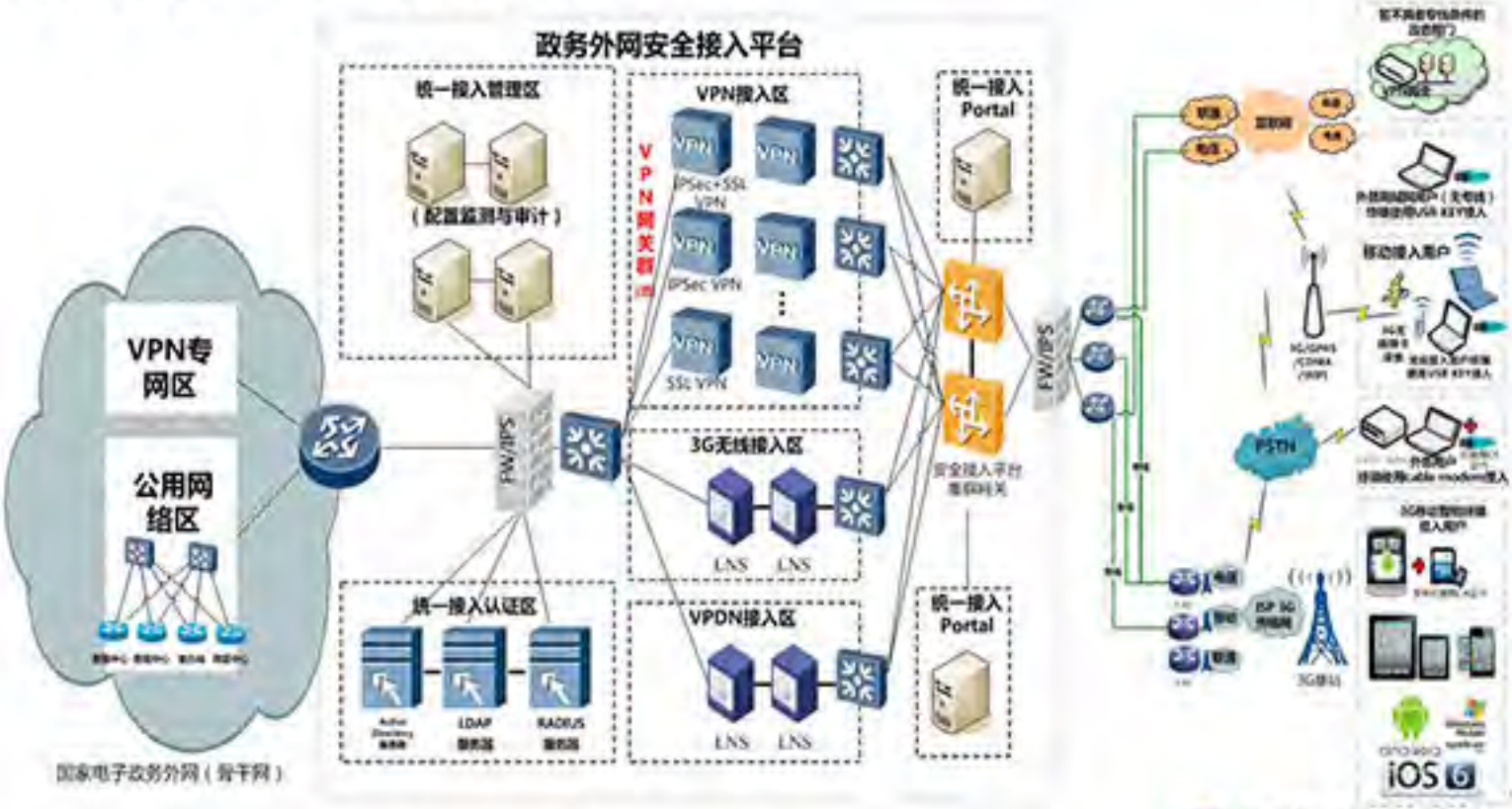
移动互联网、云计算、大数据、智慧城市、网间等安全问题思考

新技术的应用给政务外网带来的安全挑战

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

国家信息中心
State Information Center

政务外网安全接入平台



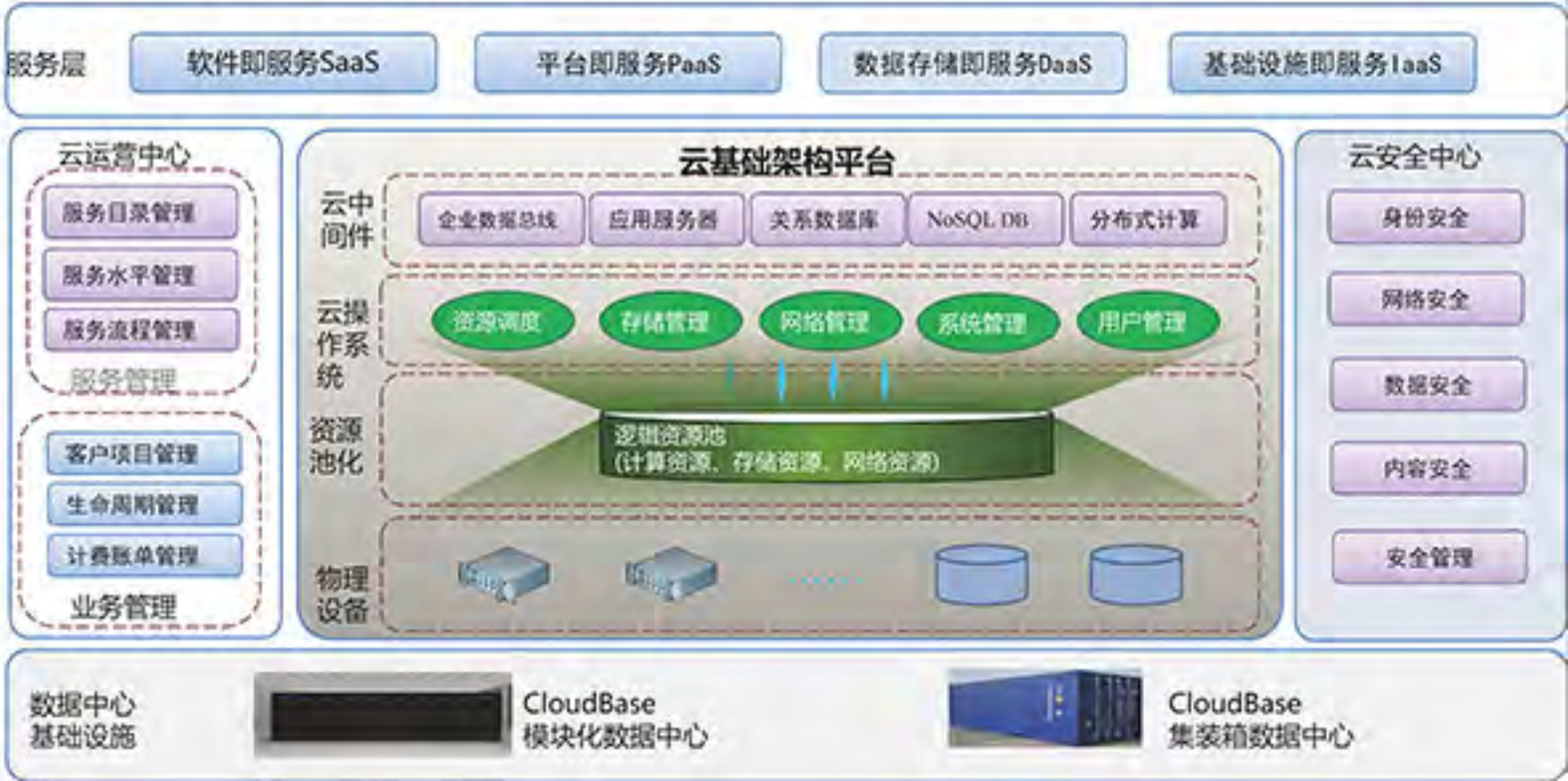
地址：北京市西城区三里河路58号　邮编：100045　电话：010-68527618 68557203　传真：010-68533919

国家信息中心
State Information Center

云计算环境的安全要求

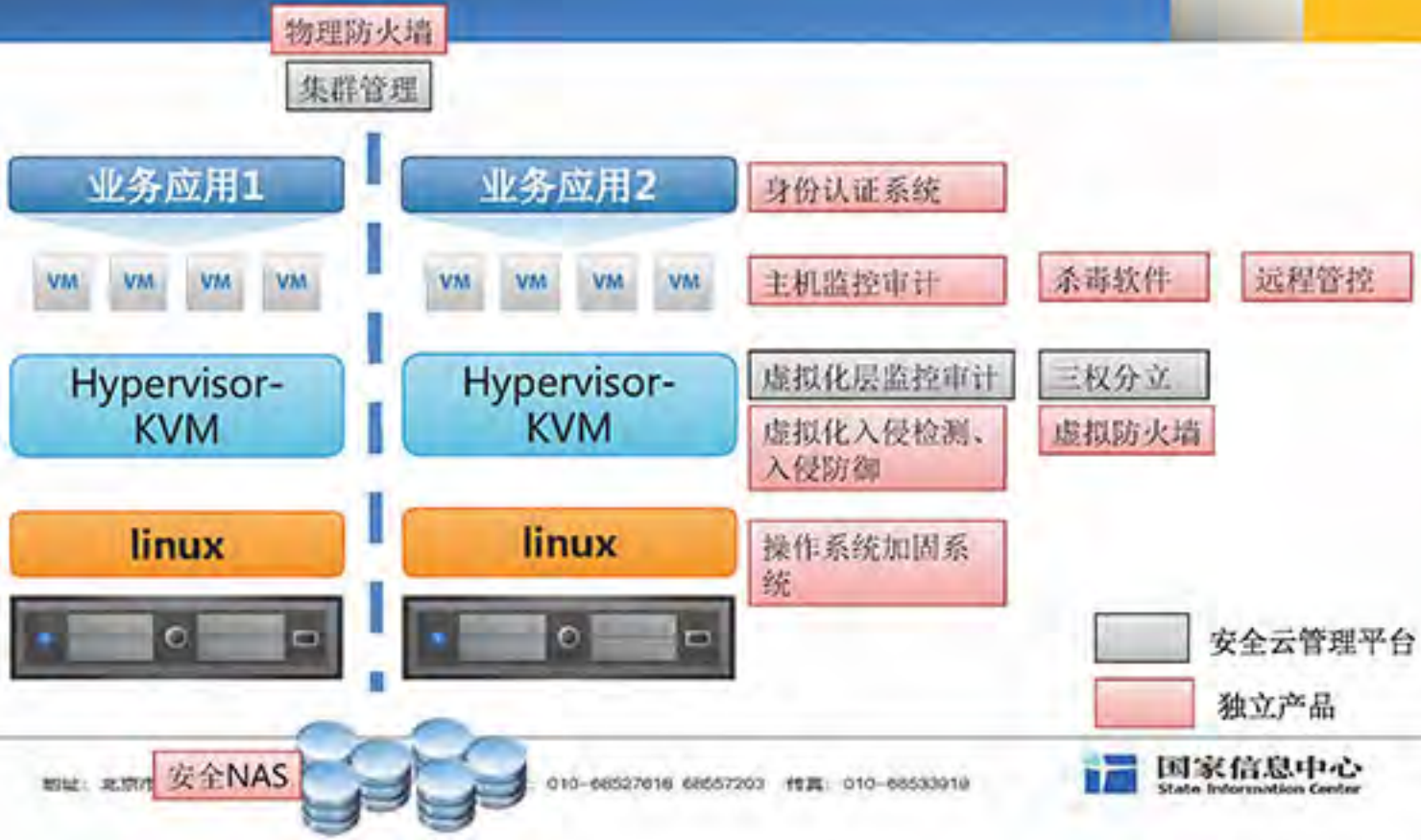
- 各地在建设云计算环境时，一定要有针对性
- 根据业务的承载情况，一定要分区域、分等级（如互联网门户网站群、内容各委局厅局的业务信息系统并能按等级保护的要求分第二级和第三级）
- 明确虚拟机之间或不同业务之间明确的边界访问控制策略
- 明确云计算环境与外部的边界安全及内部各部分之间的安全问题（如数据安全、多租户之间的安全问题、虚拟机迁移中数据证书及服务器加固等安全措施是否也随之迁移
- 多租户分级管理的要求及实现方式
- 云操作系统的管理权限分配及审计的要求
- 计算、网络及存储资源随着业务的扩大而动态分配及弹性扩展
- 开放的API接口及共用相同数据库、中间件等的具体实施方案

云计算参考架构


服务层
软件即服务SaaS
平台即服务PaaS
数据存储即服务DaaS
基础设施即服务IaaS
云运营中心
服务目录管理
服务水平管理
服务流程管理
服务管理
客户项目管理
生命周期管理
计费账单管理
业务管理
云基础架构平台
云中间件
企业数据总线
应用服务器
关系数据库
NoSQL DB
分布式计算
云操作系统
资源调度
存储管理
网络管理
系统管理
用户管理
资源池化
逻辑资源池
(计算资源、存储资源、网络资源)
物理设备
云安全中心
身份安全
网络安全
数据安全
内容安全
安全管理
数据中心基础设施
CloudBase模块化数据中心
CloudBase集装箱数据中心

云计算建设过程中应关注的安全问题

- 自建自用
  - 在任何情况下，对信息系统和数据的可管理、可控制、可追溯
  - 分区域、分等级保护是一个基本要求
  - 对云计算环境的综合管理系统和审计是关键
    - 对各类资源的实时调度时应有记录
    - 任何安全问题应实时告警
    - 对网络管理员、系统管理员、操作人员的行为审计
- 租用或托管时，作为信息系统和数据的拥有者
  - 对信息系统和数据的实时管理
  - 自主进行边界访问控制
  - 对数据的存储位置、使用情况和安全，应做到实时了解
  - 系统的运行报告、审计报告及应急措施等


物理防火墙
集群管理
业务应用1
业务应用2
身份认证系统
VM
VM
VM
VM
VM
VM
VM
VM
主机监控审计
杀毒软件
远程管控
Hypervisor-KVM
Hypervisor-KVM
虚拟化层监控审计
三权分立
虚拟化入侵检测、入侵防御
虚拟防火墙
linux
linux
操作系统加固系统
安全云管理平台
独立产品
安全NAS
010-68527616 68557203
传真：010-68533919
国家信息中心
State Information Center

什么是大数据

速度更快

第四个特征是处理速度快，时效性要求高。这是大数据区分于传统数据分析最显著的特征。

数据量大

第一个特征就是数据量大，通常为数亿、数十亿级条目数，T、P级存储容量。

类型繁多

第二个特征是数据类型特别繁多，包括网络日志、音频、视频、图片、地理位置信息等等，多类型的数据对数据的处理能力提出了更高的要求。

价值密度低

第三个特征是价值密度低，商业价值高。以视频为例，连续不间断监控过程中，可能有用的数据仅仅有一两秒。

数据准确性

在任何情况下，数据能迅速恢复使用的保障

研究机构Gartner对大数据的定义：“大数据”是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产。

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

国家信息中心
State Information Center

大数据的核心问题

- 大数据分析是今后信息化发展的趋势，目前只是起步阶段
- 在云计算环境中充分应用的基础上，实现跨系统、跨行业、跨专业、跨部门（电子政务、电子商务、企业信息系统、工业控制系统等）相关数据进行汇总、分析
- 海量数据
- 特定应用的关联分析（如智慧城市的应用）
- 个人认为：数据的质量是今后大数据分析和应用的核心问题，需要今后重点关注，如元数据的标准，异构系统的数据共享与交换等

智慧城市建设（1）

- 国家发展改革委、工信部、科技部、公安部、财政部、国土部、住建部和交通部 八部委联合发文《关于印发促进智慧城市健康发展的指导意见的通知》（发改高改[2014]1770号）--2014年8月27日印发
  - 智慧城市是运用物联网、云计算、大数据、空间地理信息集成等新一代信息技术，促进城市规划、建设、管理和服务智慧化的新理念和新模式。建设智慧城市，对加快工业化、信息化、城镇化、农业现代化融合，提升城市可持续发展能力具有重要意义

智慧城市建设（2）

- 定义：“充分利用现代信息通信技术，以全面感知、深度融合、智能协同为城市运行的基本方式，以提高城市公共管理和公共服务的效益为基本目标，以实现城市可持续发展和为人类创造美好城市生活为根本目的的信息社会的城市发展形态”

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

国家信息中心
State Information Center

智慧城市建设（3）

- 从本质来看：智慧城市本质上仍然是城市建设，因此包括了城市建设的许多方面，如政务建设、基础设施、民生建设、产业建设等
- 引入了新理念、新技术：智慧城市在传统城市建设的基础上，引入了物联网、云计算、大数据等信息技术领域的新理念、新技术和新方法。
- 特点是：从长远来看智慧城市的建设是无边界、无时间节点，将随着科技的发展而不断深化
- 最终目标：通过信息化手段，以人为本，让城市更美好，让生活更方便
- 这是一个长期的过程，现在只是起步阶段
- 智慧城市的建设取决于政务信息公开、企业和社会信息化的发展程度，各地如准备不足、条件不具备及盲目跟风等将会造成巨大浪费

网间安全问题的提出及思考

- 在网络空间中，是否存在网间安全？
- 如果有网间安全，应该如何做？应包括哪些安全措施?
- 网间安全和网络边界防护有何区别？
- 传统的数据通过路由器镜像后，对其进行监测，能起到防御作用吗？
- 在网络安全领域，我们最主要的问题是什么？（网络安全防护、网间安全、信息安全）
- 我们国家是否有一支7*24的国家队，通过网间来收集元数据，并进行实时分析、掌握来自镜外及互联网各种攻击行为，问题是，这个元数据收集点在哪？

网际安全：标准化的层次目标及关联关系

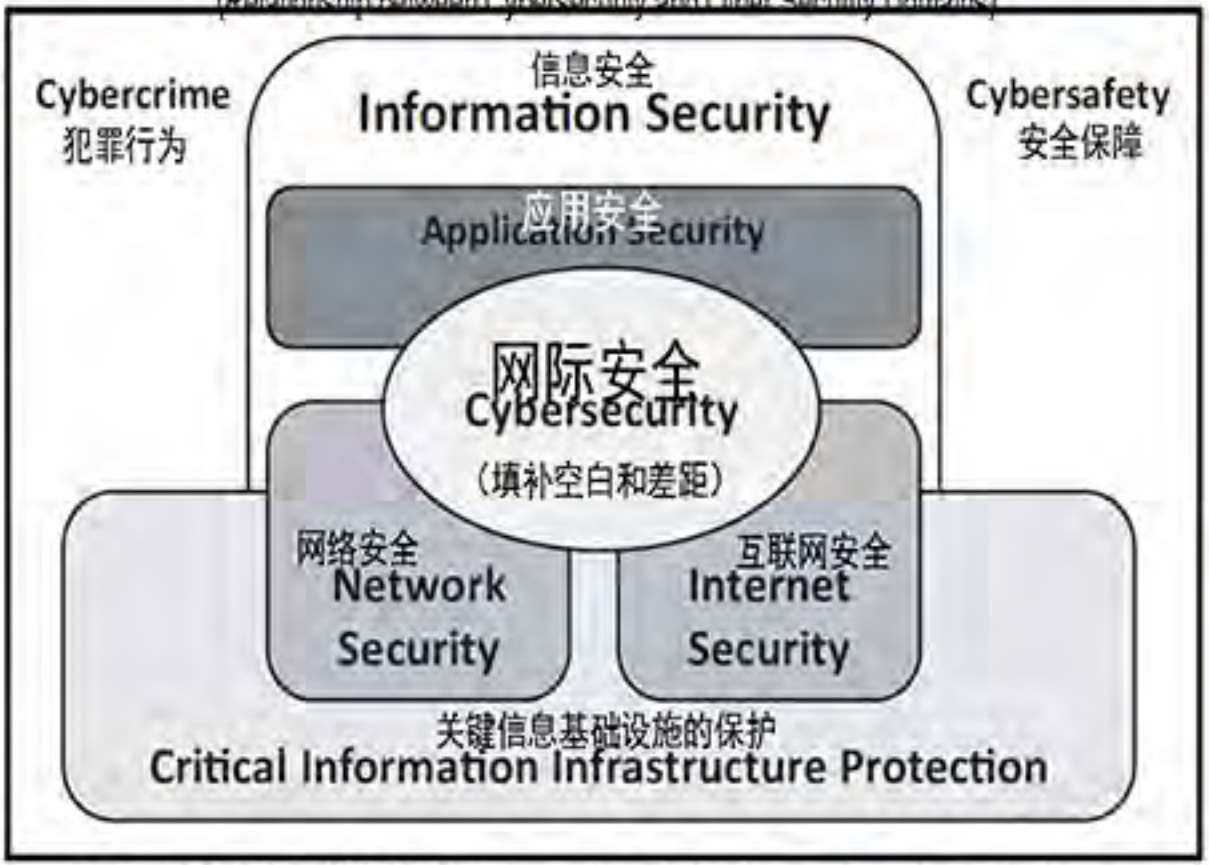
网际安全与其他安全范畴之间的关系
(Relationship between Cybersecurity and Other Security Domains)

[历史阶段：1969-1983-1990]

开放式系统
互联参考基础模型
(OSI)

7 应用层
6 表示层
5 会话层
4 传输层
3 网络层
2 数据链路层
1 物理层

ISO/IEC 7498-1:1994
"Information Technology - Open Systems Interconnection – Basic Reference Model: The Basic Model"

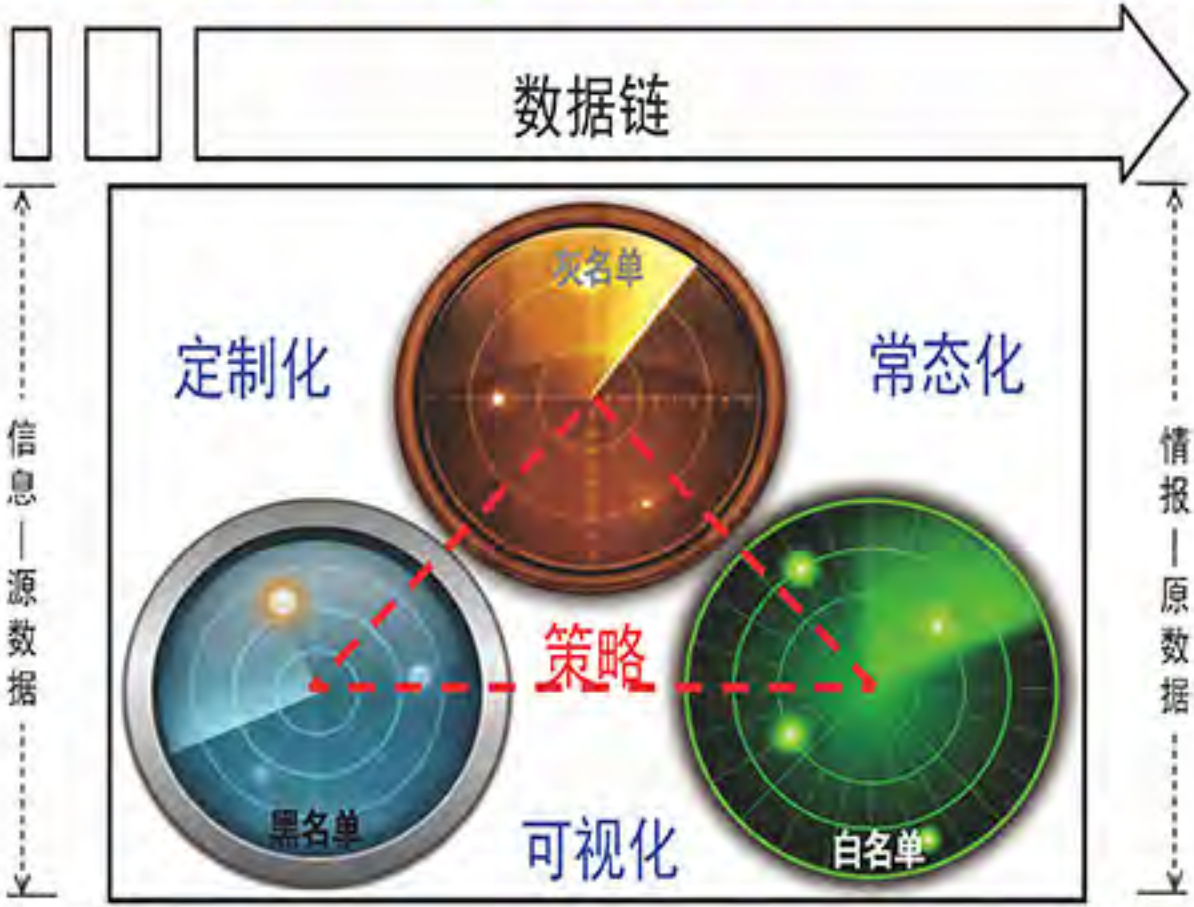


来源：ISO/IEC 27032:2012, "Information Technology – Security Techniques – Guidelines for Cybersecurity"，信息技术–安全技术–网际安全指南，国际标准化组织，2012-7

参考：网络安全纵深防御的层次体系

来源：美国国土安全部（DHS）

网际安全的路径和资源



谢謝
Thank you

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

国家信息中心
State Information Center