

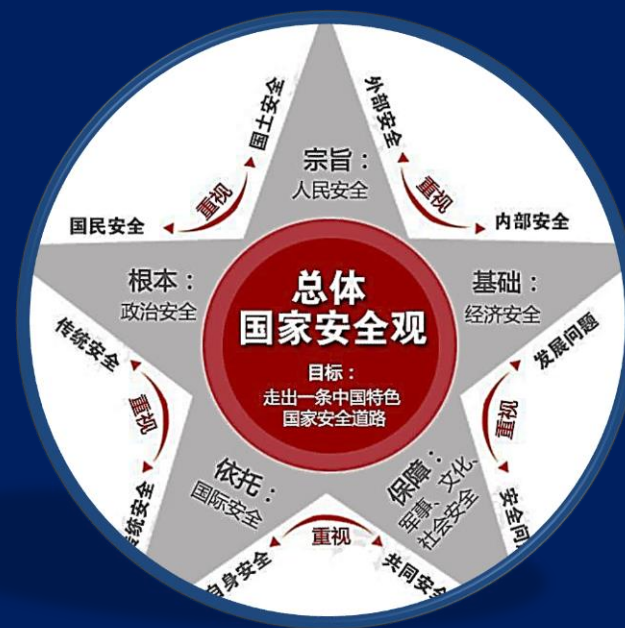
**学习贯彻《网络安全法》
扎实推进教育行业网络安全**



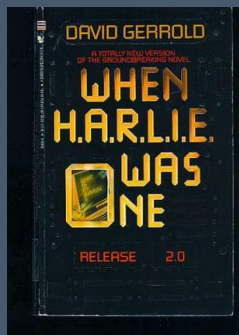
安全与 网络安全



没有网络安全就 没有国家安全



矛与盾



美国DNS服务商
遭遇DDoS攻击



乌克兰能源
部门受袭



徐玉玉
电信诈骗案



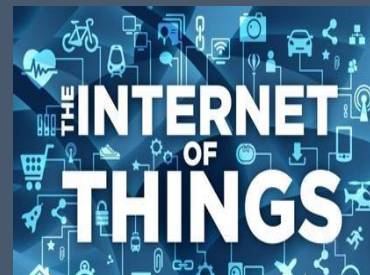
重大数据泄露



提升主动
防御能力



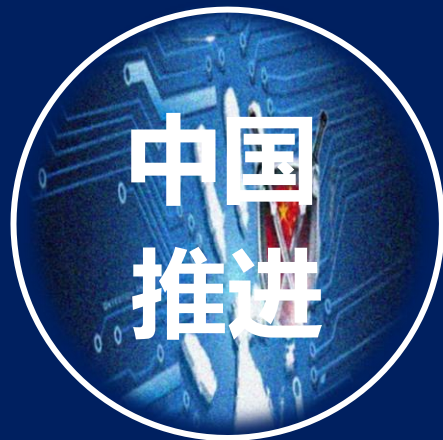
发布安全战略国家概览



重视技术研发



建立最高
协调机构



法律法规

2015.6 国家安全法

2015.11 刑法修正案九

2016.11 中华人民共和国网络安全法

规划纲要

2016.7 国家信息化发展战略纲要

政策制度

2004.9 关于信息安全等级保护工作的实施意见

2007.6 信息安全等级保护管理办法

2015-16

标准规范:

GB17859-1999 等级划分准则

GB/T22239-2008 基本要求

GB/T22240-2008 定级指南



- 全法篇幅：七章七十九条
- 网络安全定义：物理安全、运行安全、数据安全、内容安全
- 网络运营者：网络的所有者、管理者、服务提供者
- 2017年6月1日起实施

主体	总则	支持与促进	运行安全		信息安全	监测预警与应急处置
			一般规定	关键信息基础设施		
网信等有关部门	保护和监督管理	1.建立和完善标准体系； 2.推进社会化服务体系； 3.鼓励开发数据安全技术，促进开放； 4.支持教育与培训，培养人才及交流。		1.制定范围，重点保护； 2.编制规划，指导和监督； 3.组织国家安全审查； 4.组织安全抽查，应急演练，信息共享，技术支持。	履行监督管理职责，	1.建立制度，发布信息； 2.建立风险评估和应急工作机制制定应急预案，组织演练； 3.特定区域临时限制。
地方政府和有关部门	保护和监督管理	1.统筹规划，加大投入，支持研发、技术创新和应用； 2.开展经常性宣传教育。		编制规划，指导和监督。		1.建立健全制度，报送信息； 2.加强风险检测，评估预测，发布预警； 3.对事件调查评估，发布警示信息，进行约谈。
网络运营者	保障运行和信息安全		1.制定管理制度和操作规程，安全负责人； 2.编制规划，指导和监督 3.采取技术措施（防范、监测记录、数据）； 4.制定安全预案，及时处置风险，依规报告。	1.设置专门机构和负责人； 2.定期开展教育培训和考核； 3.重要系统和数据库容灾备份； 4.重要信息和数据境内存储； 5.每年一次安全监测评估；	1.严格保密，建立制度； 2.公开规则，明示目的、方式和范围，征得同意； 3.不得泄露、篡改、损毁信息，未经同意提供； 4.采取措施确保安全，依规报告 5.建立投诉和举报制度。	采取措施消除隐患
个人或组织	遵守法律、秩序、公德，不得危害安全。		1.提供真实身份信息； 2.不得非法入侵，窃取数据。		1.有权要求删除、更正信息； 2.不得发布有害和违法犯罪信息； 3.不得发送恶意程序和违法信息。	



重视程度大幅提升

责任制度逐步建立

启动网络安全监测



政策体系初步形成

全面推进等级保护

提升应急响应和通报能力

现状



50万所



1800万人



26000万人



22万所



45万个



38000万条

特点

机构多

人员多

系统多

数据多

关注度高

影响面广

重视 程度

2013

部长专题办公会，明确了部内责任分工

2014

制定加强教育行业信息技术安全工作方案
出台教育行业网络和信息安全工作的指导意见

2015

第一次部党组会，专题听取信息技术安全汇报
网络安全写入2015年教育信息化工作要点
网络安全经费首次纳入部本级经费预算

2016

第十九次部党组会，专题听取网络安全工作汇报
网络安全工作写入教育信息化“十三五”规划
网络安全写入2016年教育信息化工作要点

10月26日，成立教育部网络安全和信息化领导小组
11月7日，召开领导小组第一次会议，专题研究网
络信息安全工作，防止师生信息泄露。



重点任务

加强教育行业网络与信息安全工作的指导意见

领导体系 (第八条)

成立教育部网络安全和信息化领导小组

分级管理, 逐级负责, 明确责任分工

主体责任、领导责任、信息系统安全责任

管理制度 (第21、32、52条)

等级保护制度 (第三章)

联合公安部全面推进信息安全工作

组织开展部属单位信息安全等级保护工作

教育行业信息系统安全等级保护定级工作指南

安全防护能力 (第21、25、34条等)

漏洞、病毒、攻击、侵入、灾备、加密

监测应急处置 (第五章)

建立信息通报机制

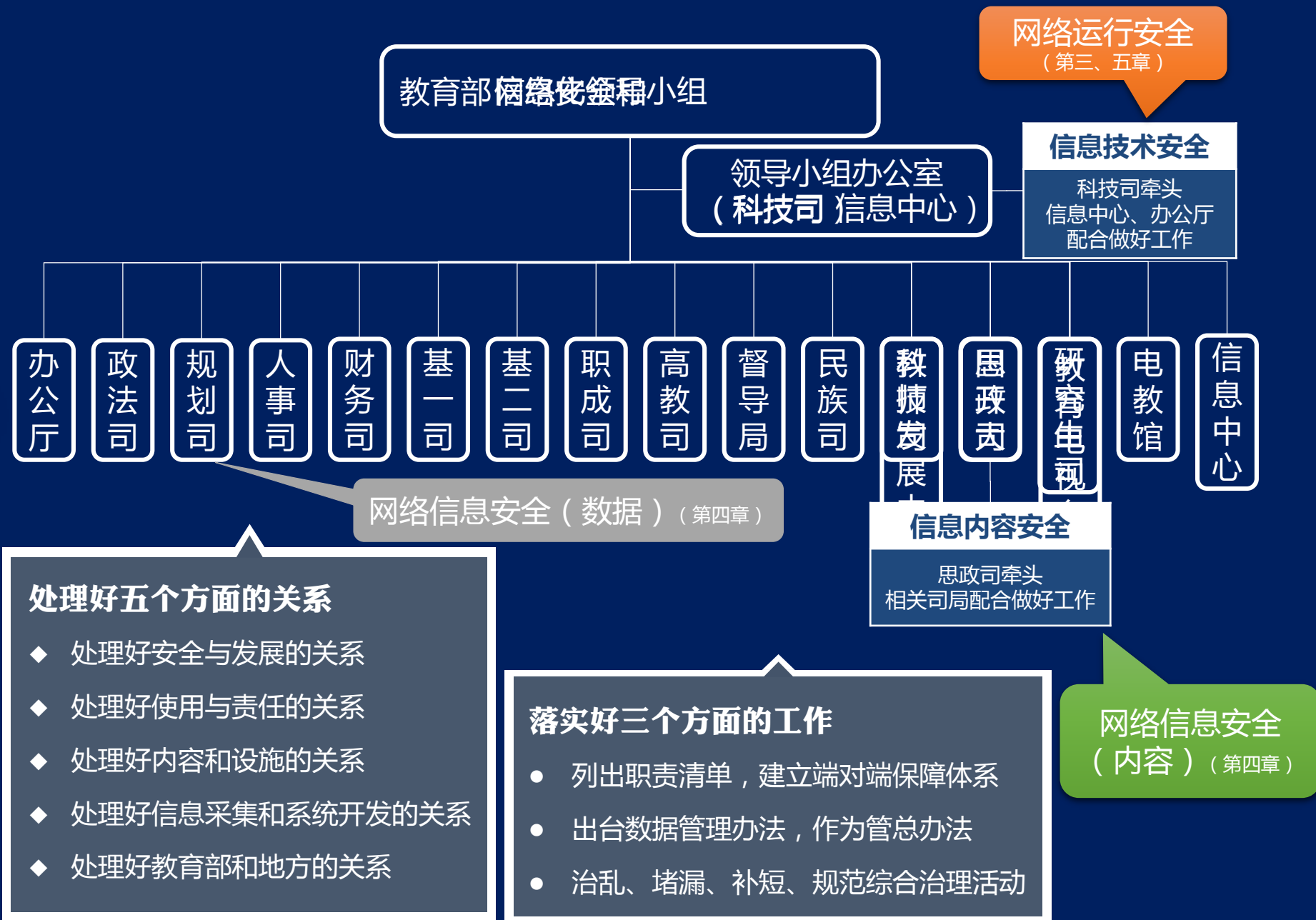
启动信息系统安全监测预警

发布信息技术安全事件报告与处置流程

人员培训 (第19、34条)

组织信息技术安全培训班

标准规范 (第15条)



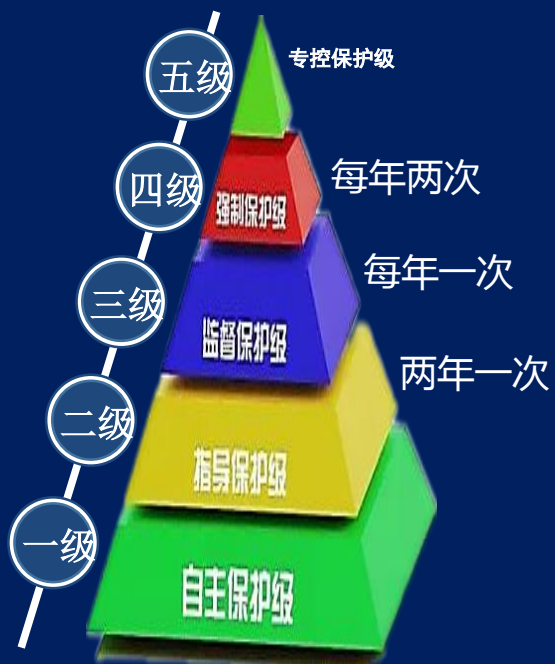


省级统筹

教育部统筹



等级保护



目标:

2016年底基本完成教育行业信息系统的定级、备案和第三级以上信息系统的测评、整改工作。

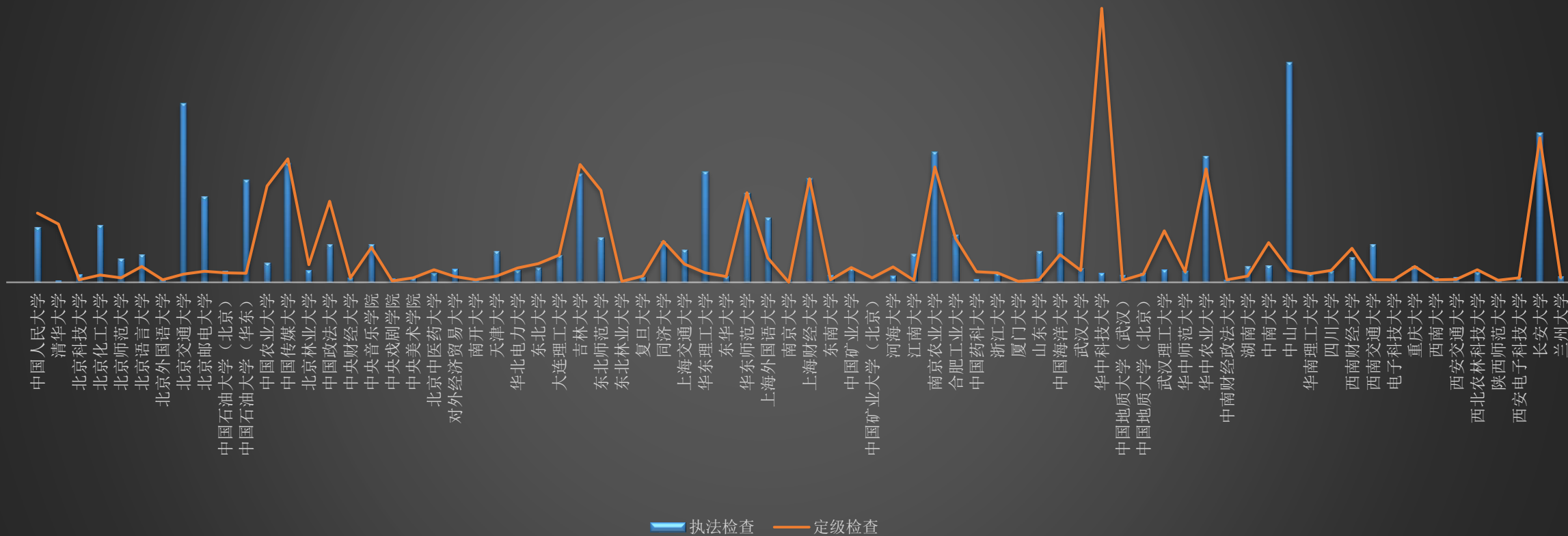


关键信息基础设施



等级保护

知识百科



安全监测



网络安全威胁

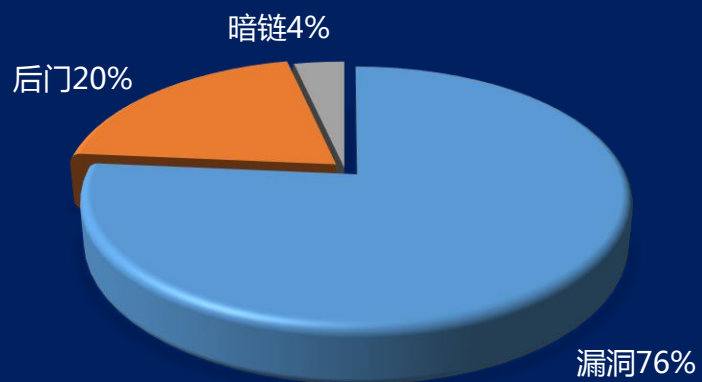
- 漏洞监测
- 后门监测
- 暗链监测
- 钓鱼网站监测
- DOS攻击监测



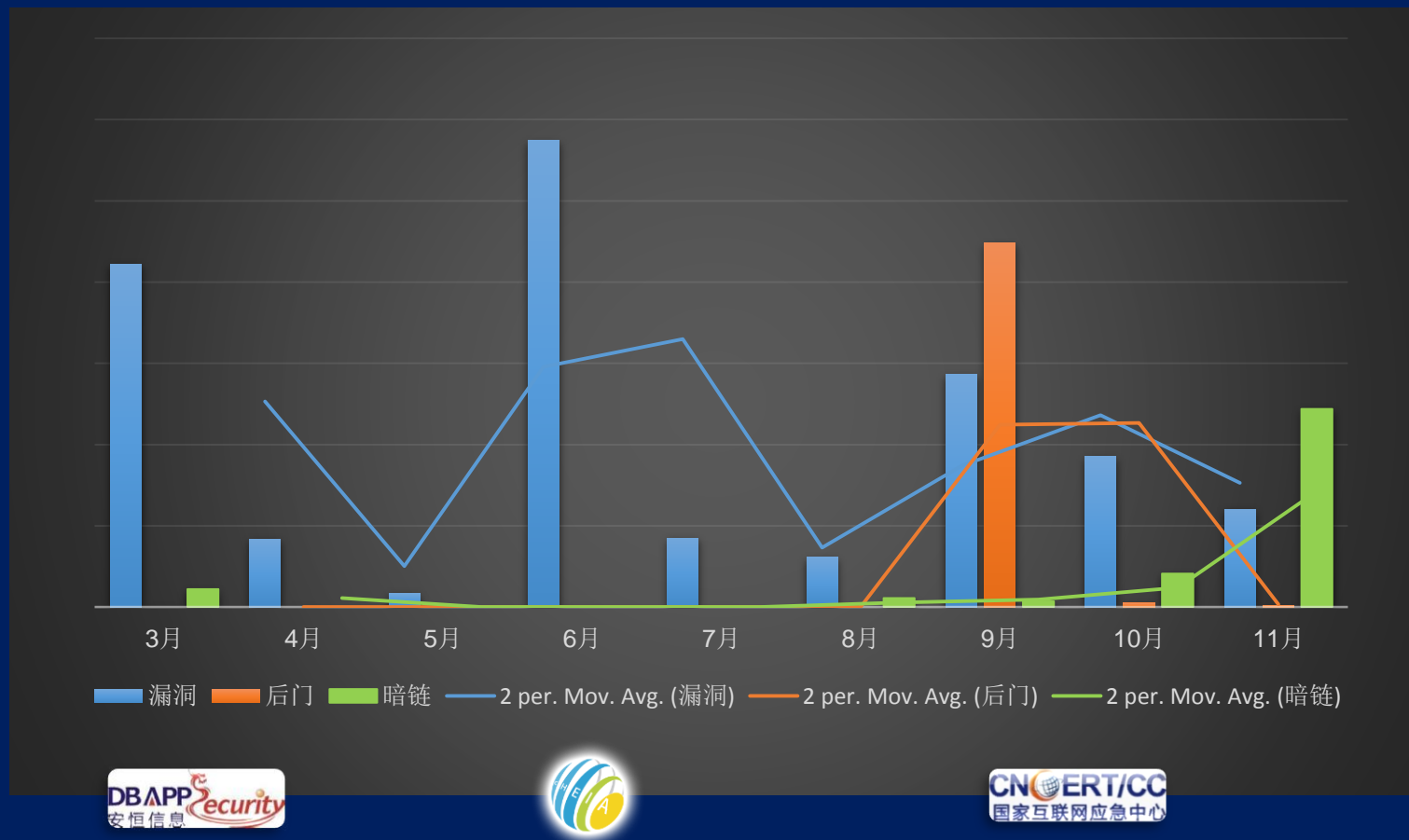


威胁分析

总体情况



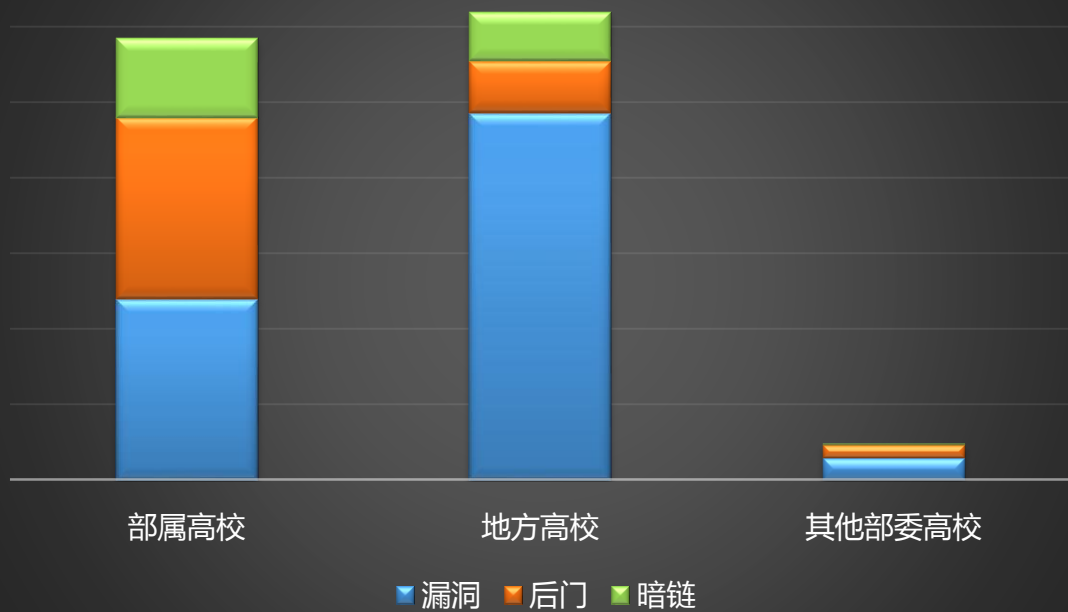
安全威胁



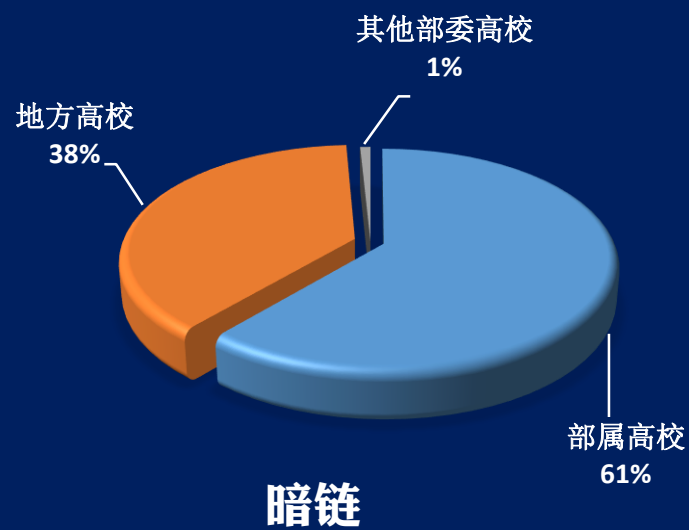
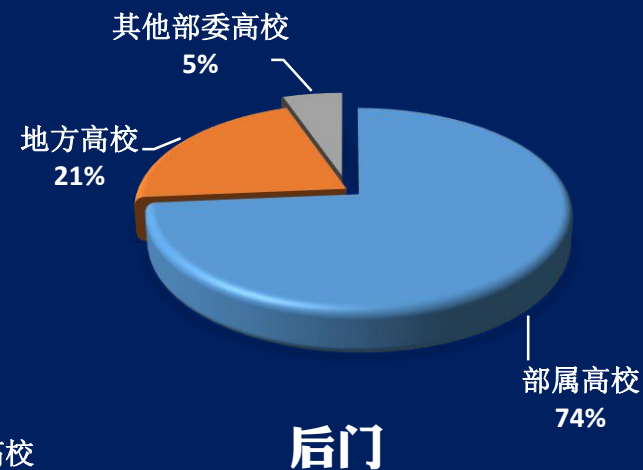
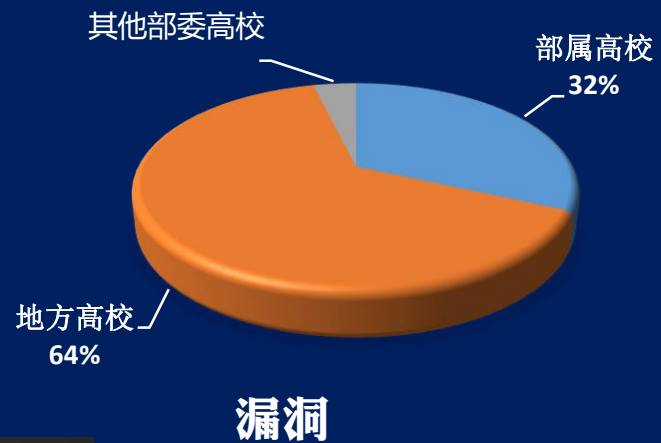


威胁分析

高校分类



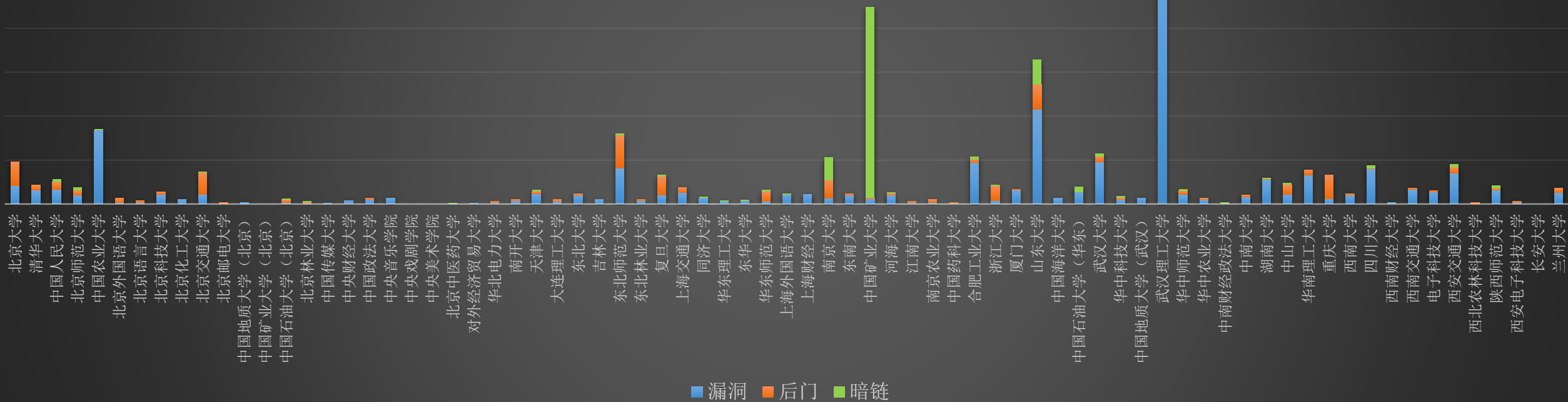
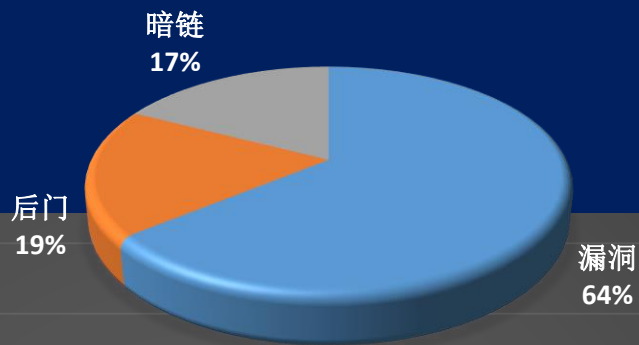
安全威胁





威胁分析

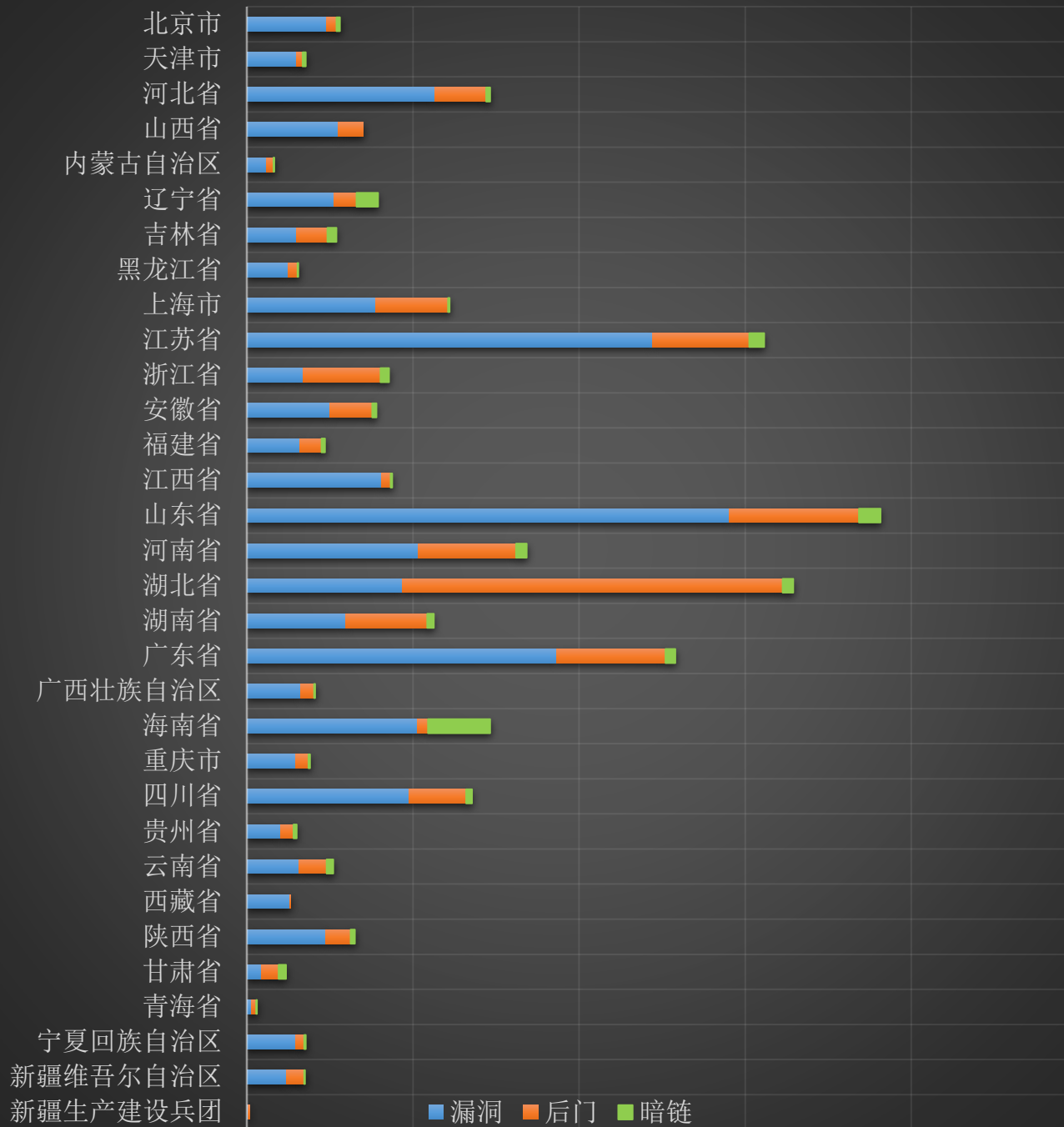
部属高校





威胁分析

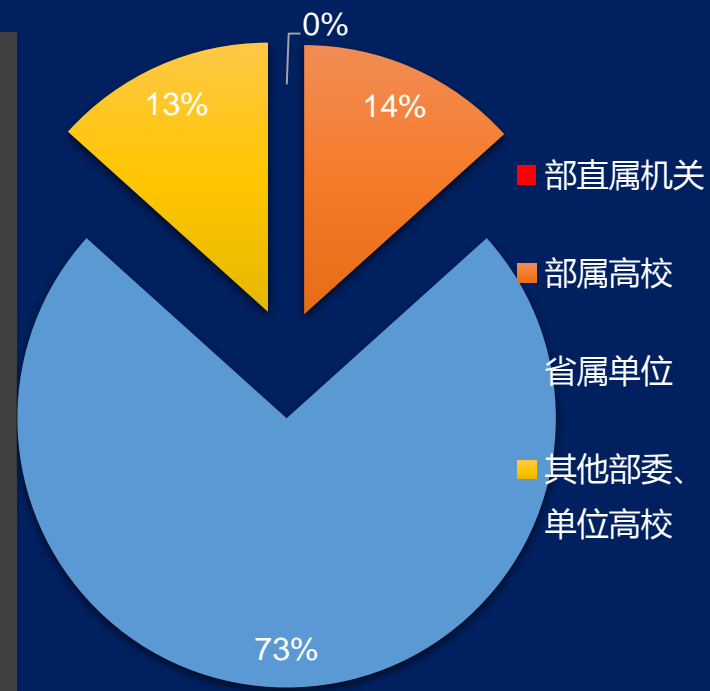
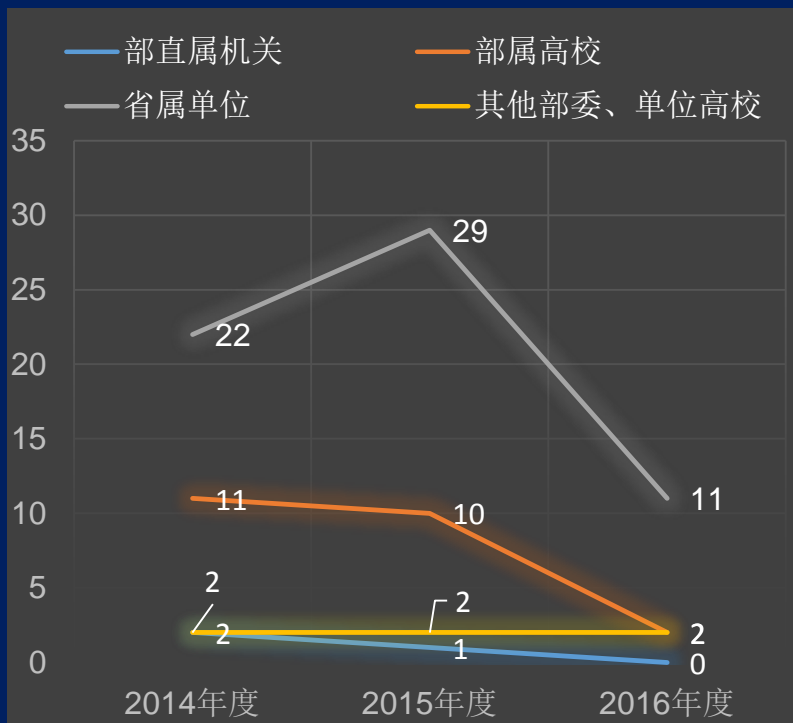
分省情况





应急响应及通报机制

- 加入了国家有关通报机制
- 建立了机关、直属单位、部属高校、省级教育行政部门在内的联络机制
- 明确了安全事件报告和处置流程
- 对安全事件进行应急处置
- 对工作不利的单位进行通报





思想认识不到位

规定动作不到位

数据管理亟待加强



责任意识缺失

信息系统小散乱

安全防护能力急需加强



提高认识，主动作为 认真学习贯彻《网络安全法》

- 学习和宣传《网络安全法》
- 梳理网络运营者责任和义务
- 对照本单位现状制定方案.....

扎实落实重点工作

- 加强和理顺管理体制
- 建立健全网络安全管理制度
- 加快落实网络安全等级保护制度
- 确定关键基础设施并落实责任
- 开展网络安全监测预警
- 提升应急响应和处置能力.....

采取管用好用的措施

- 发挥工作组作用，开展信息共享
- 与各地网信、公安、CERT开展合作
- 签订网络安全承诺书
- 开展网络安全自查.....

关口前移，与信息化统一部署

谢谢！

