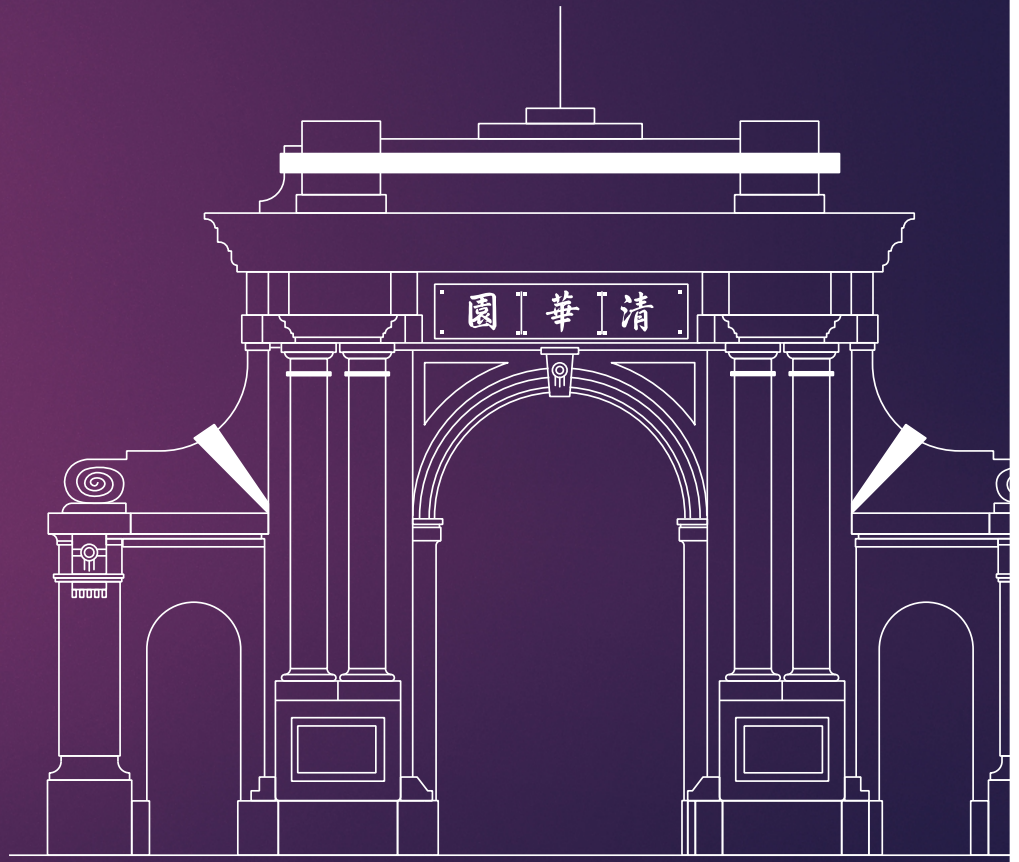
清华大学
信息化安全保障体系



清华大学信息化技术中心 姚星昆

2021年3月26日

目录

- 高校网络安全形势和面临问题
- 近年清华采取网络安全措施

高校网络安全形势和面临问题

上级部门要求

- 要求学校做好网络安全工作，将网络安全工作评价结果纳入教育部对学校及领导班子的考核
- 要求全面梳理单位网站和信息系统基本信息，完成“双非”网站排查整治工作
- 信息系统（网站），特别是关键信息基础设施，应确保安全隐患清零后方可上线，要求专人专岗24小时值守

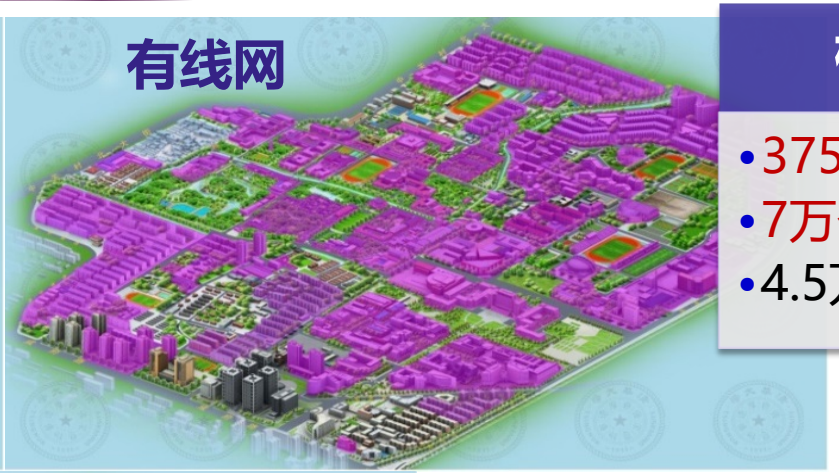
- 门户网站、电子邮件系统和重要对外服务网站，应在做好重点防护的基础上保障访问畅通

加强电子邮件工作统筹，规范电子邮件账号管理，保障电子邮件系统安全运行等提出明确要求

清华大学信息化：网络基础设施

校园无线网

- 190座楼宇
- 1.3万个热点
- 3.5万个并发在线终端



校园有线网

- 375座楼宇
- 7万个有线端口
- 4.5万个并发在线终端

通信管井网络

- 1.1万芯公里光纤
- 1100个通信管井

电视+电话

- 3万个有线电视端口
- 3.2万部固定电话

清华大学信息化：信息系统和数据中心


数据中心

信息系统 + 数据中心

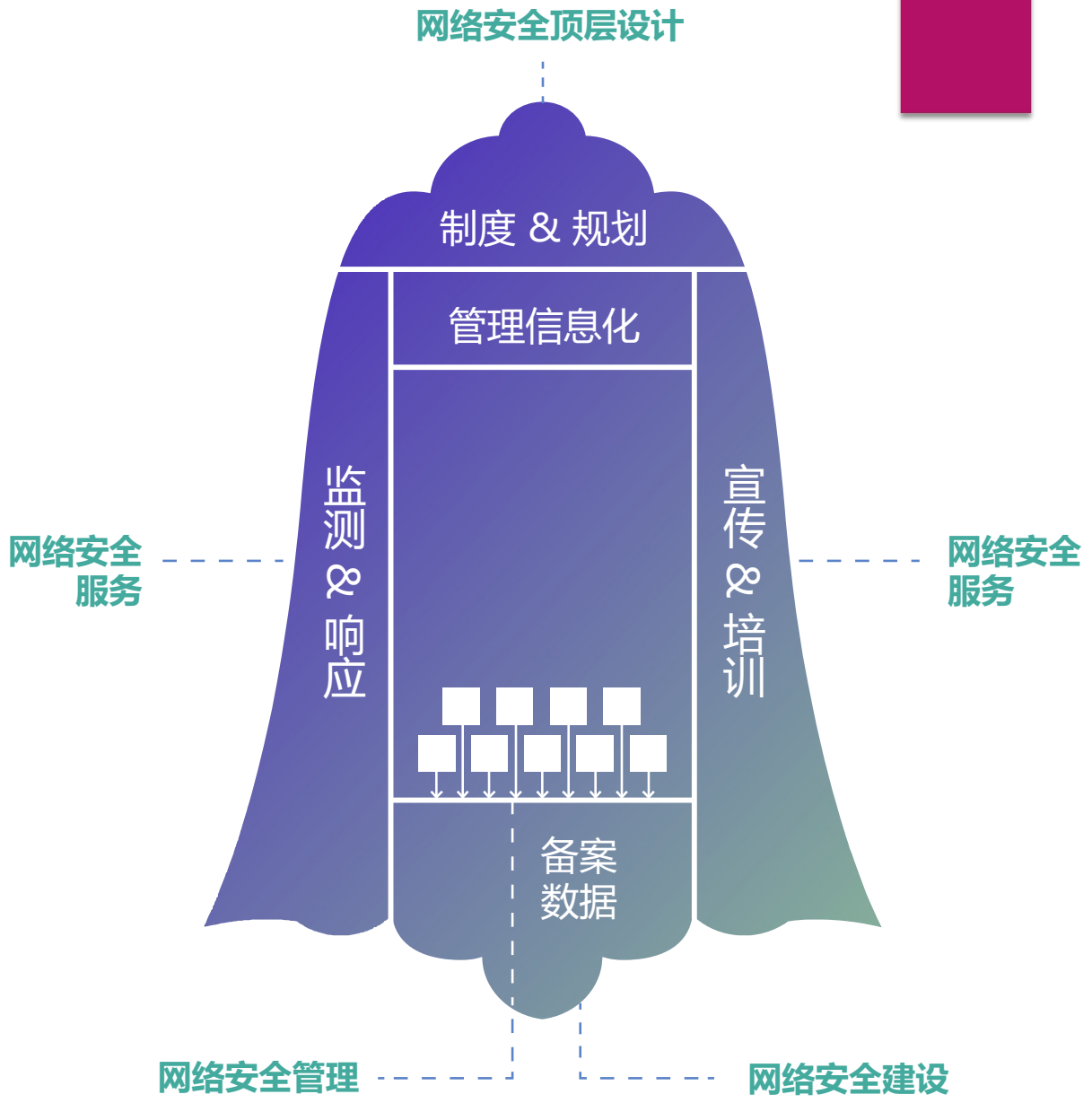
- 全校79个单位的331个业务系统
- 数据存储量13 PB
- 支撑全校信息系统的硬件设备800多台套

矛盾与转变

- **两个矛盾**
  - 国家和上级部门日益增长对网络安全监管力度与高校自身发展现状的矛盾
  - 现代大学日益增长的信息化建设需求与高校网络安全投入的矛盾
- **两个转变**
  - 从网络安全的应急处置，到加强日常的网络安全建设
  - 从单纯依赖采购部署安全设备提高防护能力，到强化管理通过内涵式发展全方位打造防护体系

清华大学
信息化安全
保障体系

金钟罩

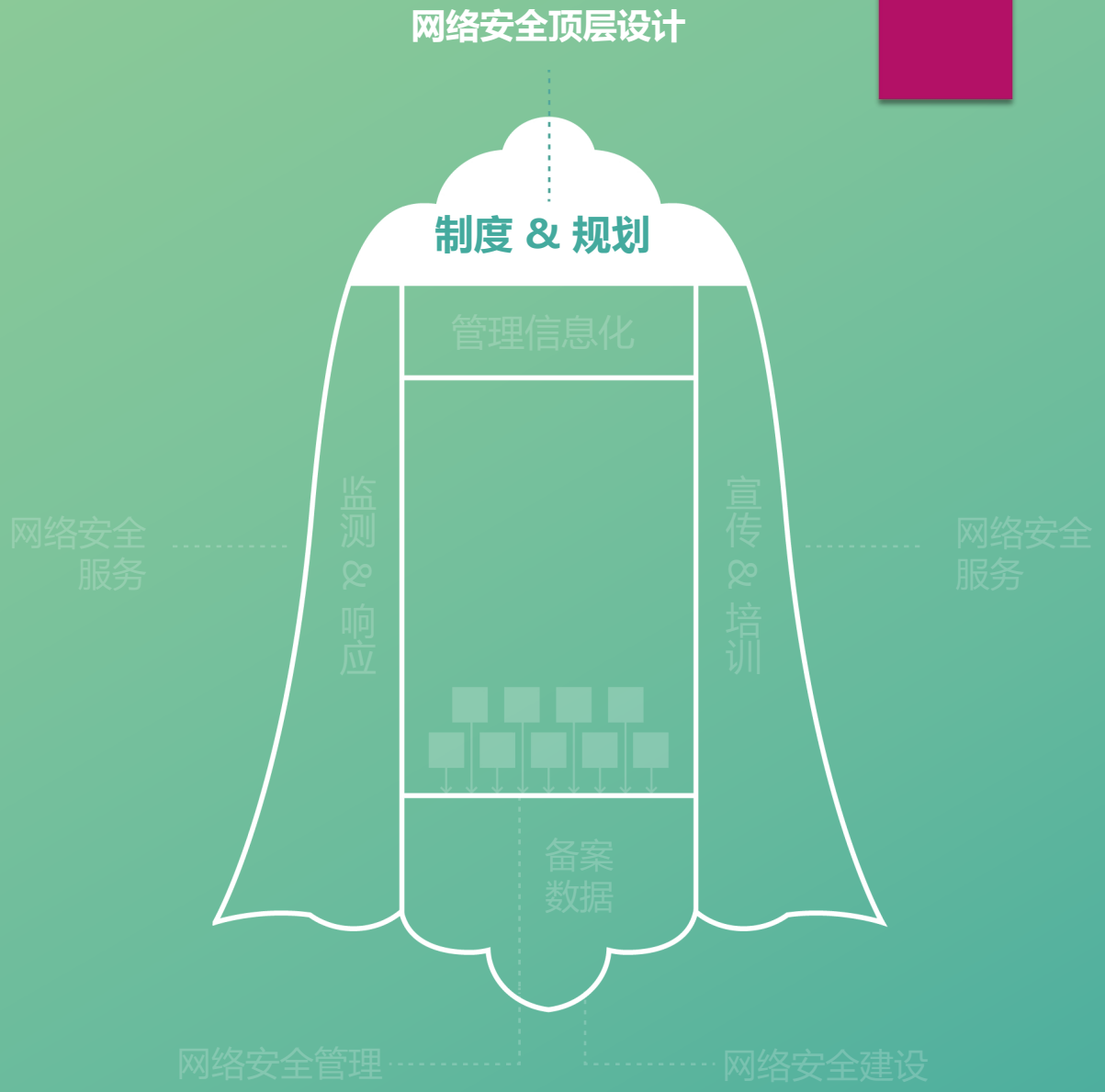


近年清华采取网络安全措施

措施

01

网安工作体系建立



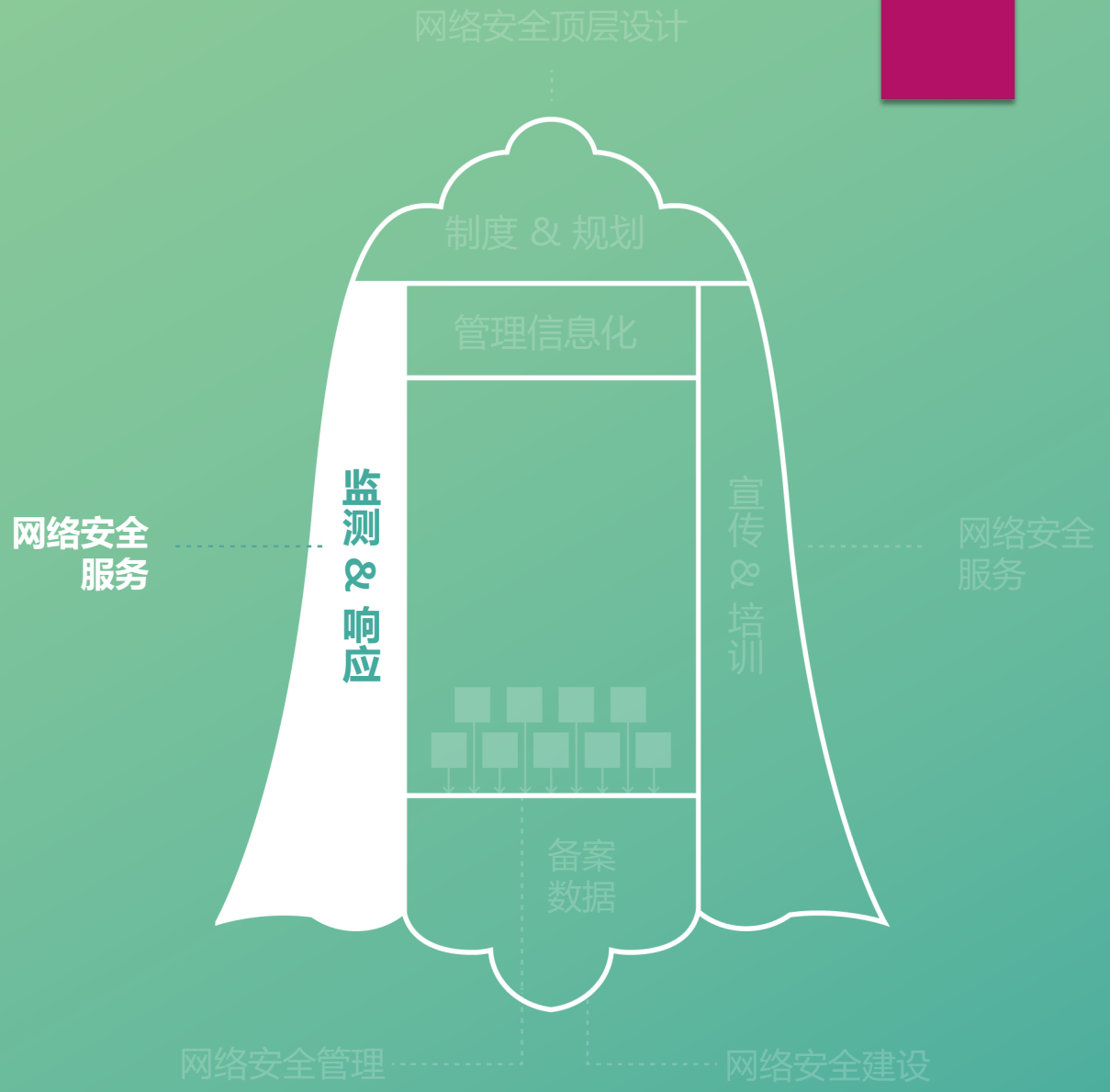
网络安全工作体系建立

- 网络安全管理系列文件颁布实施
- 设立网络安全专项经费
- 网络安全涉及业务均可在线办理，OA与业务系统数据联动
- 明确党委书记和部门负责人为各单位第一责任人，并指定一名网络安全工作联络员，承担本单位网络安全日常管理和具体落实协调工作
- 明确信息办和中心的分工与合作机制

措施

02

信息系统隐患排查



校外安全通报

收到来自教育部、北京市公安局、网安大队、行业平台等有关部门通报安全隐患

校内安全检测

每年春秋两季由学校自己发起对全校备案数据的网络安全检测

网络安全整改通知书

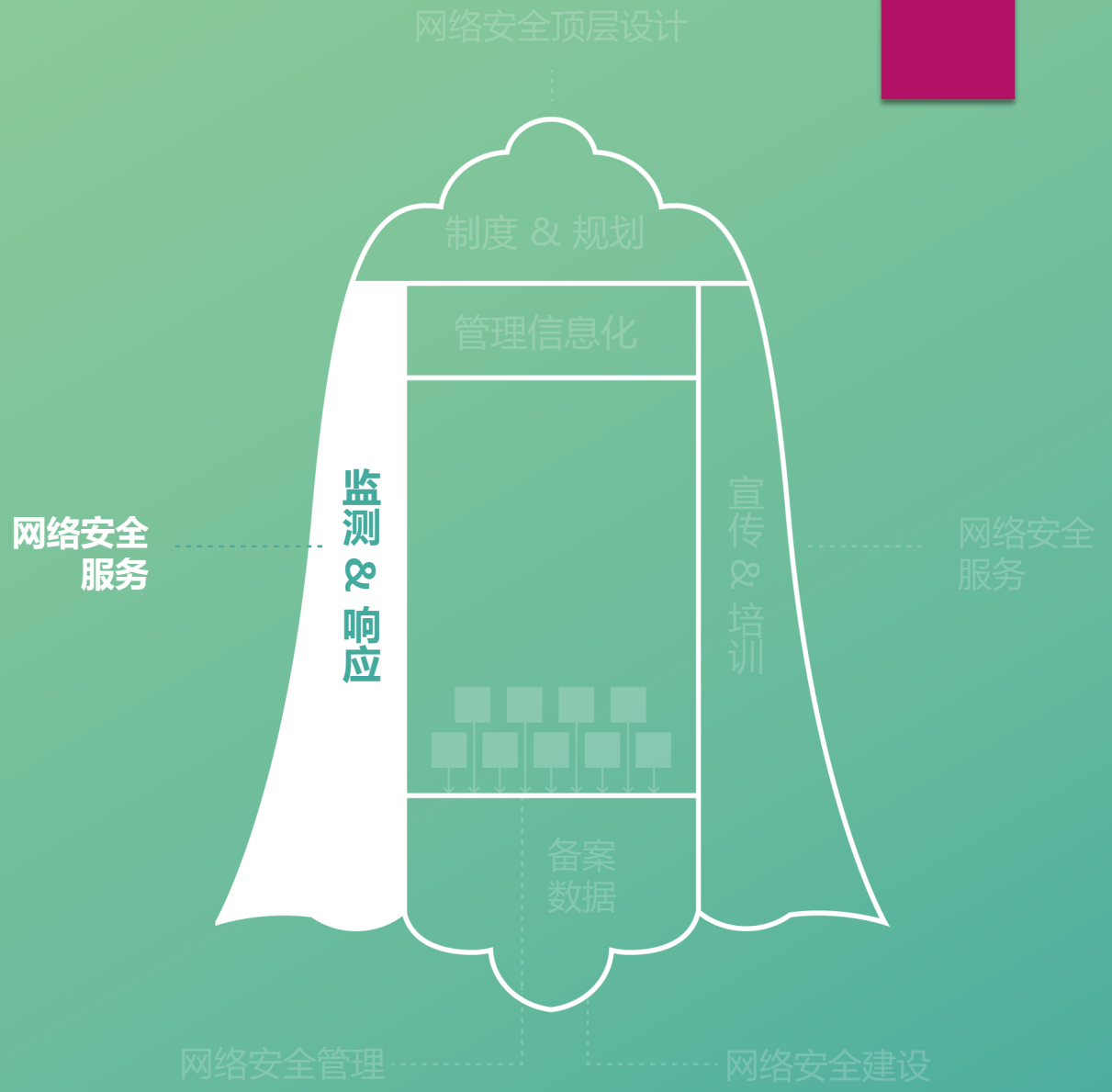
根据漏洞的高/中/低危来处置，分别为5/10/15天，分限制校内访问/下线

网络安全整改情况，纳入学校年底单位绩效考评

措施

03

网安应急预案演练



网络安全
应急预案

升级全校网络安全应急预案

细化二级单位处置四步工作法

应急预案
演练

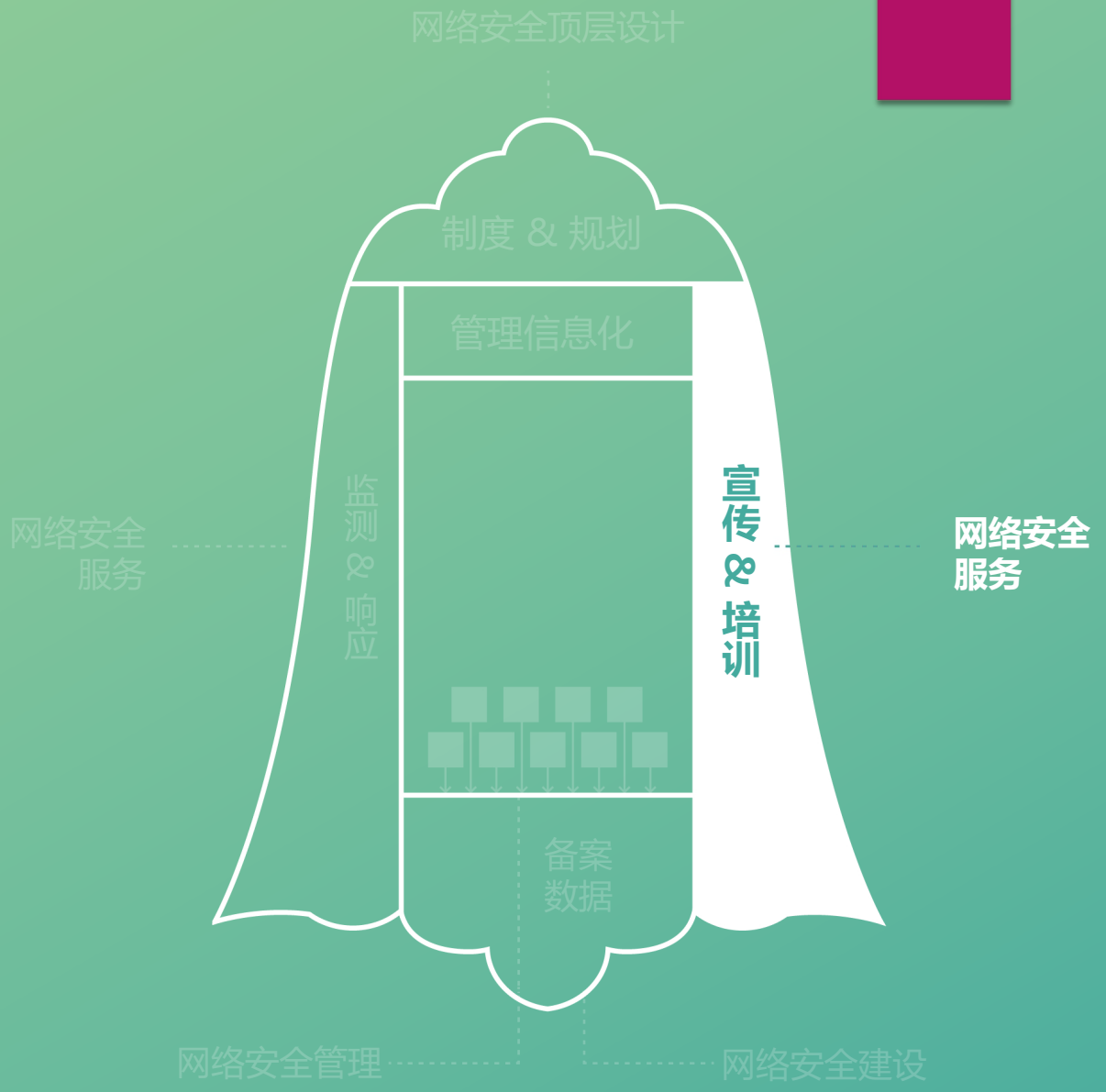
演练网站被恶意篡改

演练校园网受到拒绝服务攻击

措施

04

网络安全宣传培训



网络安全
宣传培训

在所有的网络安全措施中，
是投入最小效益最大的

宣传培训要多层面多维度，
针对不同主体采取不同形式

宣传培训
目的

统一思想、取得共识、落实行动、同步推进

到各院系
开展网络安全宣传培训

生命学院、图书馆、计算机系、
航院、社科学院……

“国家网络安全宣传周”
系列宣传教育活动

一门课程、一场报告、一项赛事、
一次巡展、公众号推送









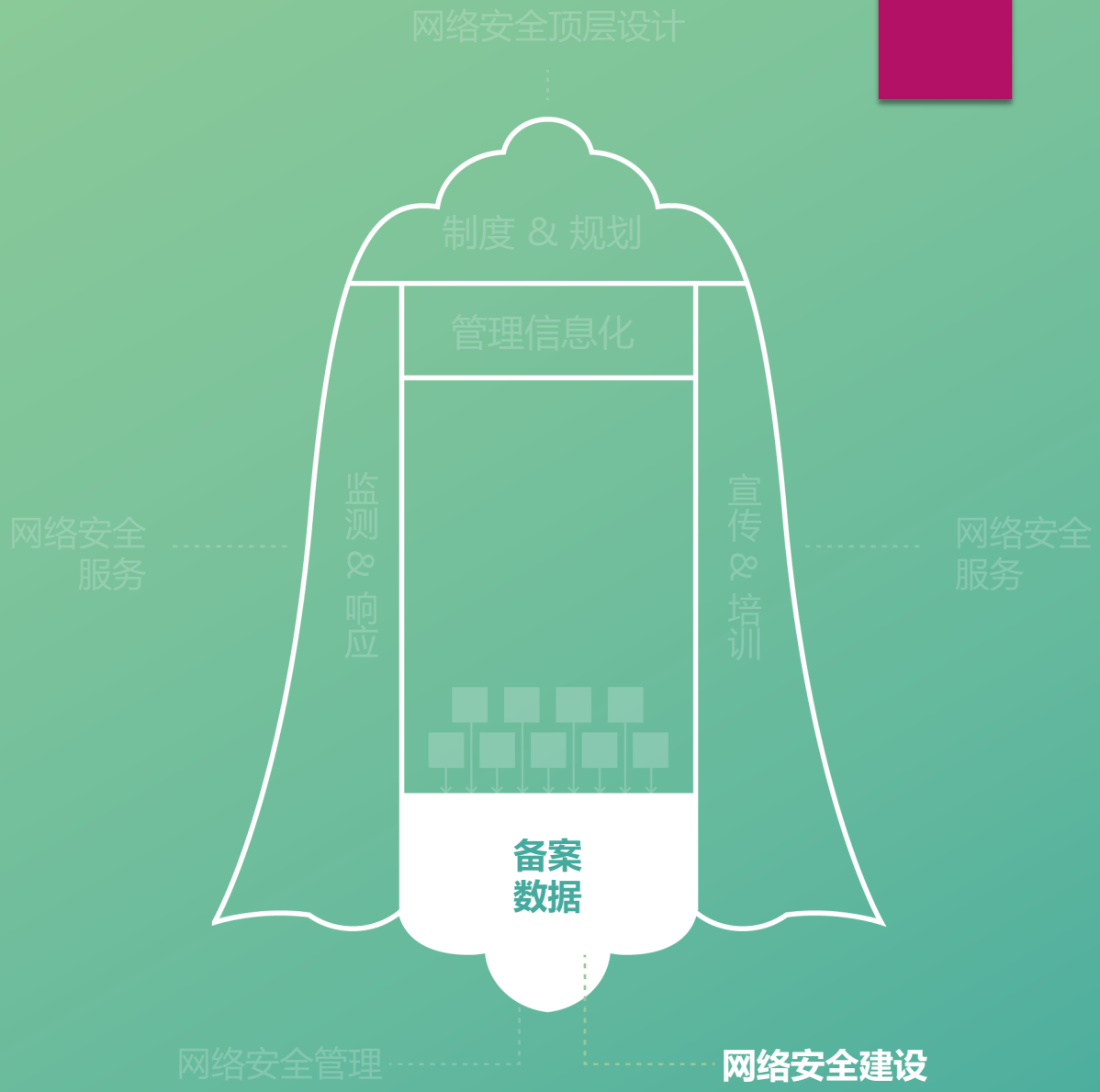

9:20
2021年度网络安全培训课程（2）
1 / 16
2021年度网络安全
培训课程
信息化工作办公室
信息化技术中心
不懂
收藏
评论
9:20
网络安全培训课程_预览
成员
习题集
讨论区
分组
学习日志
全部
课堂
课件
试卷
公告
线上学习
3月24日 星期三
16 : 57 课件
2021年度网络安全培训课程（2）
16 : 29 课件
2021年度网络安全培训课程（2）
2月25日 星期四
11 : 05 课件
2021年度网络安全培训课程（1）
2月22日 星期一
13 : 56 课件
2021年度网络安全培训课程（1）
9:20
网络安全培训课程_预览
2020
11月30日 星期一
16 : 40 课件
2020年度网络安全培训课程 （10）
11 : 39 课件
2020年度网络安全培训课程（10）
11月25日 星期三
10 : 04 课件
2020年度网络安全 培训课程
10月30日 星期五
15 : 02 课件
2020年度网络安全培训课程（9）
9月29日 星期二
10 : 42 课件
2020年度网络安全培训课程（8）
9月14日 星期一


清华信息化
2019年5月16日 下午12:25
网络安全提示：微软发布Windows高危漏洞
Windows高危漏洞！快来...快来.....了解一下！
清华信息化
2019年5月22日 下午12:07
清华云盘 你的安全保障
清华云盘，你的安全保障！
清华信息化
2019年9月6日 上午9:56
邮件安全那点事（中）
清华信息化
2019年9月4日 下午4:46
邮件安全那点事（上）
安全无小事，大家要提高警惕，做好邮件安全防护！
清华信息化
2019年9月11日 上午9:38
邮件安全那点事（下）
清华信息化
2019年10月17日 上午11:27
电脑又稳又强的秘密（下）
工欲善其事，必先利其器，手把教学如何让你的电脑又稳又强。
清华信息化
2019年9月26日 上午11:32
WiFi有风险，蹭网要当心！
在蹭网的背后,存在着令人惊叹的安全隐患，大家需提高警惕，文明用网络。

措施

05

信息系统备案清查



“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。”

---习近平总书记4.19重要讲话

为什么要信息系统备案清查？

1. 事前预防：纳入学校统一监管，提前预警，防止出现安全事件

2 .事中发现：根据情报匹配备案数据，提前部署应对危机

3 .事后处置：出现问题第一时间下线，协助单位定位问题，联动处置

措施

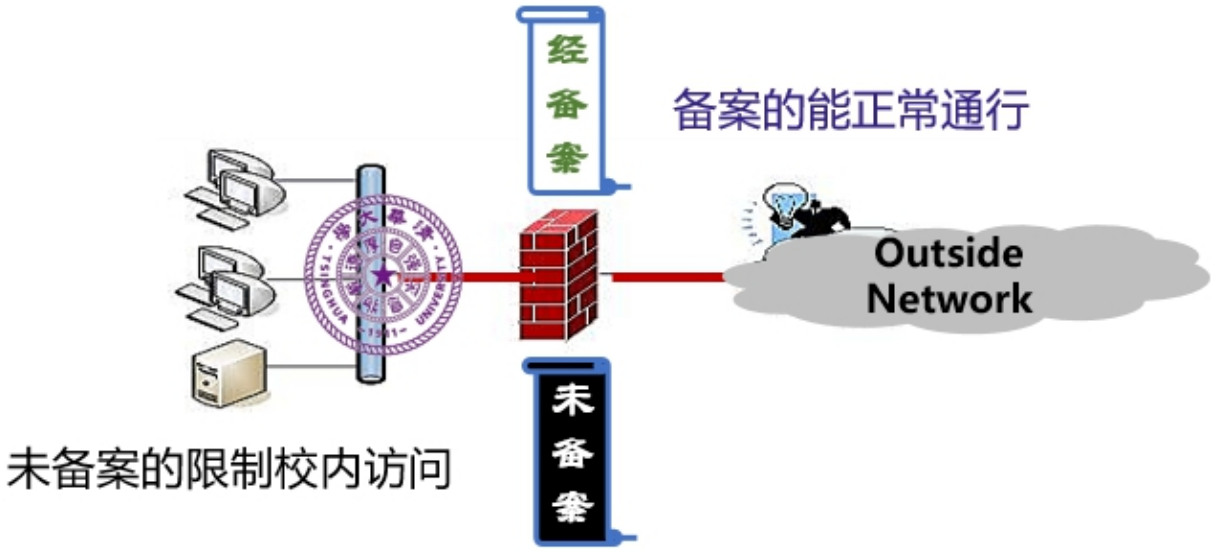
06

信息系统强制备案

信息系统强制备案

2019年9月18日起，在校园网内实施信息系统强制备案管理机制

凡未按要求完成备案的信息系统将被限制为校内访问



措施

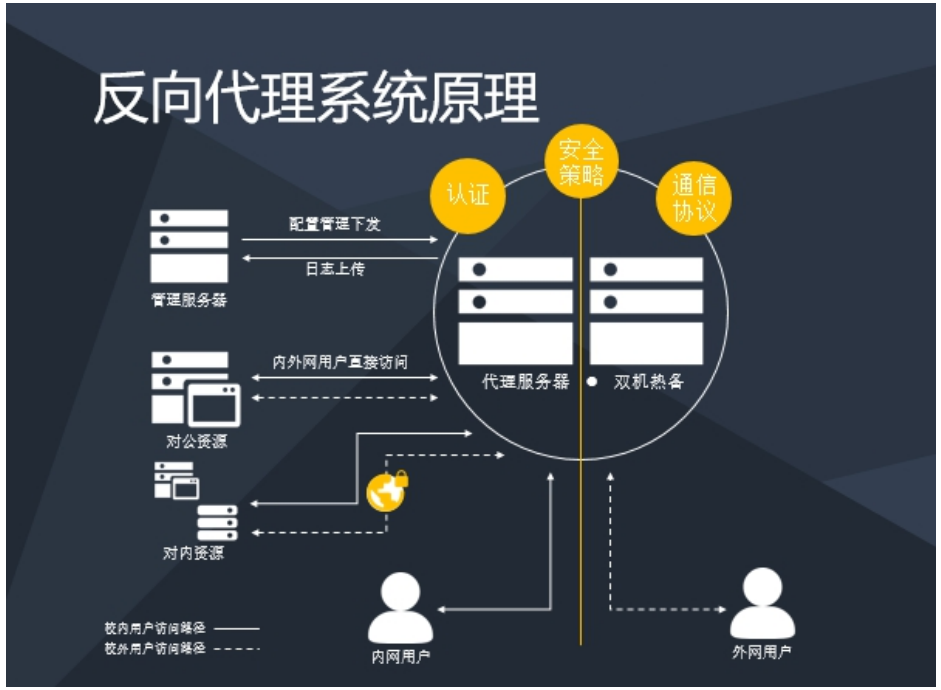
07

对备案网站实施反向代理

实施反向代理

对外提供WEB服务的系统和网站实施反向代理，实现对网站集中管控和安全防护

反向代理部署采取负载均衡，可靠性更强



措施

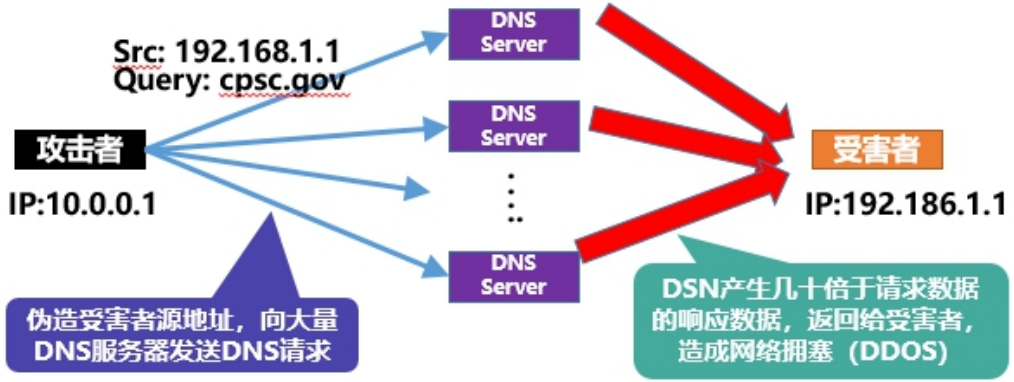
08

全校域名一级解析

全校域名一级解析

清理全校二级单位自建DNS服务器，杜绝DNS放大攻击

DNS作为一种以UDP为主的服务协议，攻击者可以很容易伪造受害者源IP造成DNS放大攻击, 造成网络瘫痪



措施

09

全校电子身份年审

全校电子身份年审

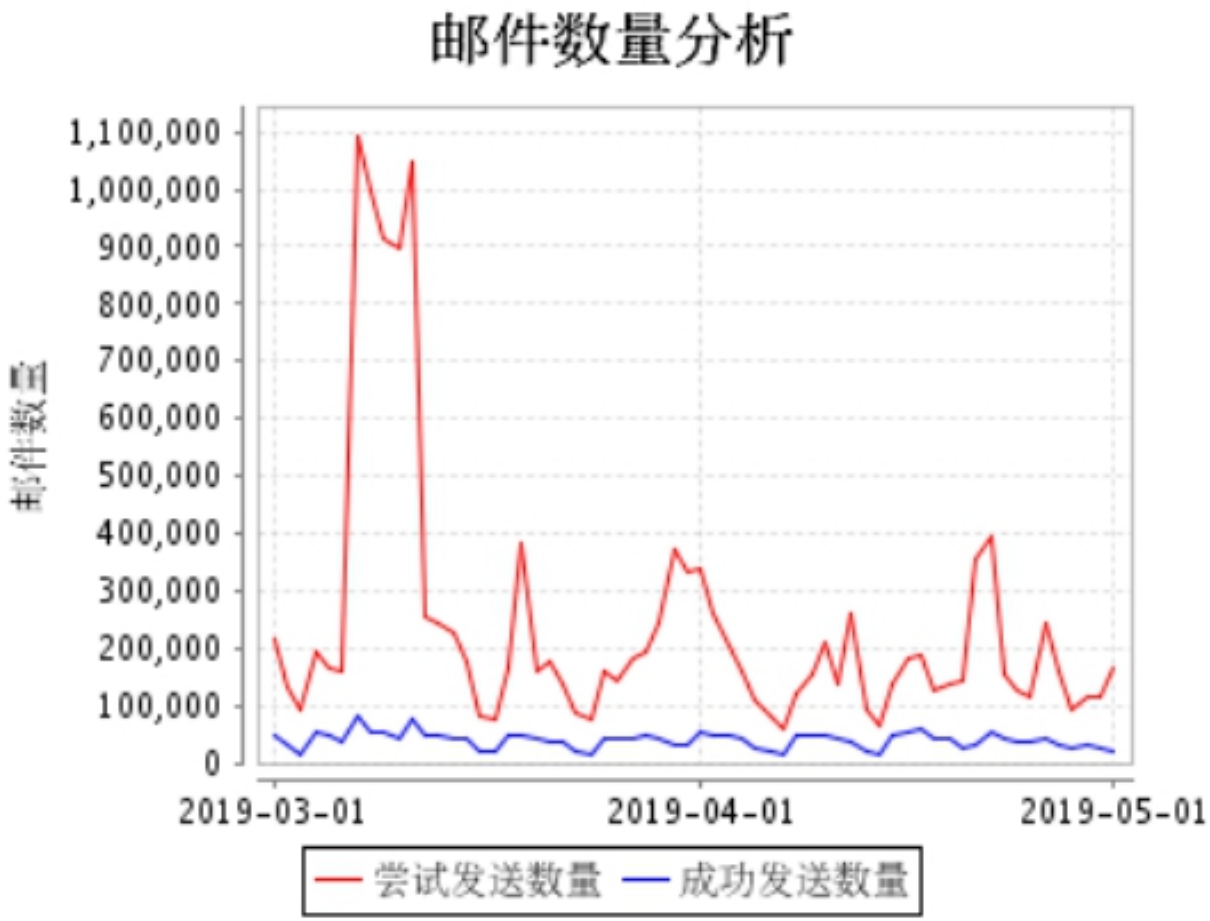
每年4月1号开展为期两周的年审工作，近5万师生修改个人密码

电子身份年审目的

加强统一身份认证平台的用户管理，检查弱口令，清理僵尸用户，设置统一身份认证防范暴力破解策略

电子身份年审
安全效益

红色是尝试外发邮件数量，在4月1号启动电子身份年审之前，很明显有一次邮箱被盗用，向外发送大量垃圾邮件的情况，4月之后基本平稳



措施

10

电子邮件安全治理

校级邮件系统升级

制定邮箱治理专项方案，升级学校邮件系统

- 电子邮件日均发送数21.84万封,其中站内互发18.8万、发站外3.04万

二级单位邮件系统处置

对19家二级单位邮件系统逐一协商量身定制，全部完成

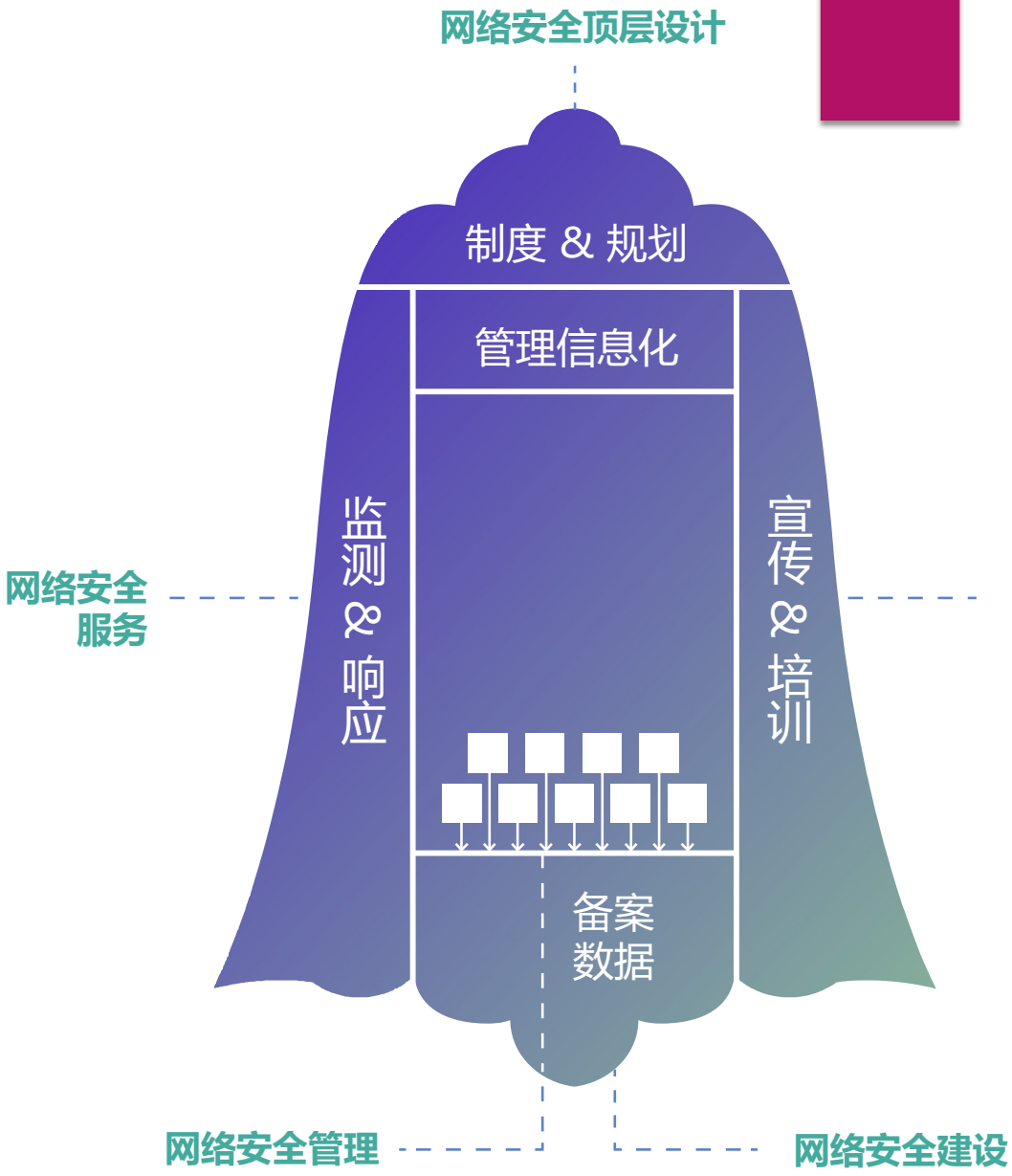
- 同意迁移到学校或者弃用11家、租用类3家、外地/独立法人单位5家

技管并重 管理先行

管理要有更多的责任和担当，为技术的落地穿针引线，铺路搭桥，为技术的实施争取更大的共识，创造更好的舆论

内涵式发展

通过向内发力打造我们的信息化安全体系，全面提升网络安全防护能力



感谢支持！