北京外国语大学
BEIJING FOREIGN STUDIES UNIVERSITY

重保时期网络安全工作实践

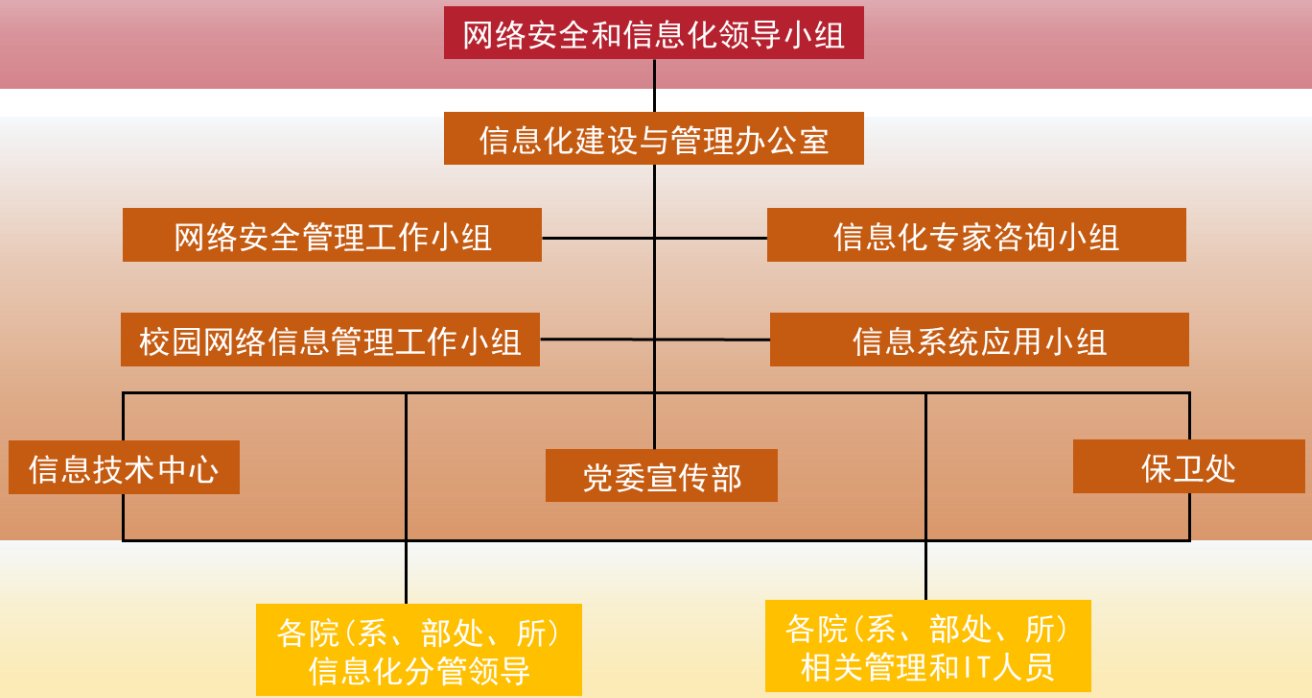
——北京外国语大学网络安全工作交流

汇报人：杨红波

时间：2022年6月

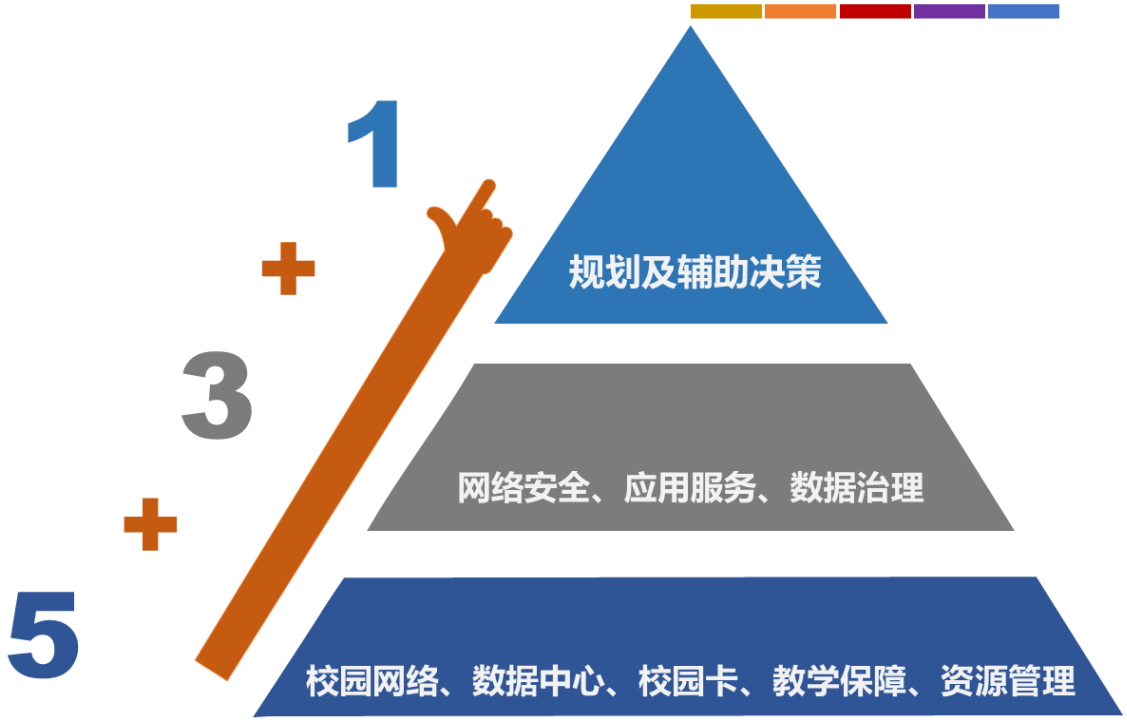
关于北外信息化

北外信息化组织机构



2020年4月14日第14次党委常委会修订领导小组名单

关于数字北外



高级信息化服务

重点信息化支撑

基础信息化支撑

信息技术中心简介

历 史

北京外国语大学信息技术中心是学校教育信息化的主要推动者，中心的历史可以追溯到1950年，目前已有60多年的历史。

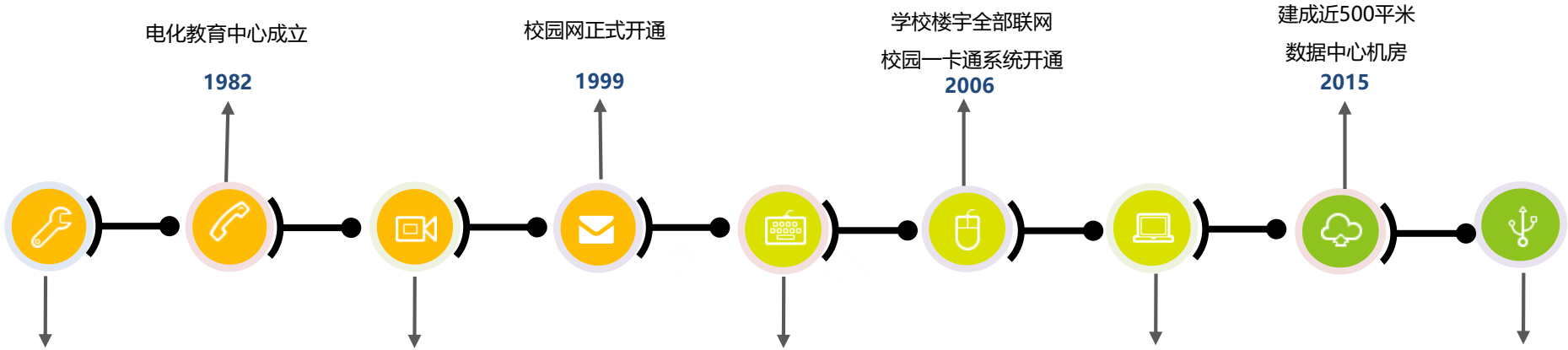
重要发展节点

1982年随着电化教育大楼落成，学校成立独立建制的电化教育中心；1997年学校成立网络中心；

2008年随着信息技术的发展，为了更好地推动资源整合、发展转型，更好地服务于教学、科研，原网络信息中心与原教育技术中心合并成立信息技术中心。

北京外国语大学 BEIJING FOREIGN STUDIES UNIVERSITY

信息技术中心发展历程



主机时代　网络时代　互联网时代

北京外国语大学 BEIJING FOREIGN STUDIES UNIVERSITY

北京外国语大学
BEIJING FOREIGN STUDIES UNIVERSITY

目录 CONTENTS

01

政策指引和实际需求

政策指引和实际需求

不断做强做优做大我国数字经济

《求是》2022年2月刊 发表习近平总书记文章

- 党的十九大提出，推动互联网、大数据、人工智能和实体经济深度融合，建设数字中国、智慧社会。
- 党的十九届五中全会提出，发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。
- 国家出台了《网络强国战略实施纲要》、《数字经济发展战略纲要》。
- 新冠肺炎疫情暴发以来，数字技术、数字经济在支持抗击新冠肺炎疫情、恢复生产生活方面发挥了重要作用。
- 加快新型基础设施建设、推进重点领域数字产业发展、完善数字经济治理体系。

2022年1月4日，北京冬奥会、冬残奥会主媒体中心

政策指引和实际需求

教育部举行党组理论学习中心组集体学习暨教育信息化首场辅导报告会

怀进鹏在讲话时指出：

- 习近平总书记高度重视信息化建设和数字经济、数字中国建设发展，多次强调**数字化、网络化、智能化**在中国特色社会主义现代化建设中的重要意义。
- 教育系统要深入学习领会，认真贯彻落实，**把教育信息化作为发展的战略制高点，以教育信息化推动教育高质量发展，以教育信息化引领教育现代化。**
- 要牢牢把握“**方法重于技术、组织制度创新重于技术创新**”的工作理念，按照“**应用为王、服务至上、示范引领、安全运行**”的工作要求和思路一体化推进建设与应用。

2022年2月，教育部

政策指引和实际需求

目前教育行业的建设的信息化阶段基本完成，步入加速发展的数据化时代，多维度创新方兴未艾。未来，数据和智能技术将全方位加码教育行业的的决策、服务和治理模式，迎来教育发展的智能化阶段。

教育数字化转型以云计算、大数据、人工智能、物联网、区块链等数字技术为支撑，**信息安全和数据安全为数字化转型提供安全保障**。

国家、教育部、公安文保等工作要求

政策指引和实际需求

2016年-2021年，随着《网络安全法》、《等保2.0》、《个人信息保护法》《数据安全法》密集发布，网络安全监管合规要求越来越严厉。

2016年

- 2016.04习近平主席发表网信重要讲话
- 2016.07国务院办公厅印发《国家信息化发展战略纲要》
- 2016.08中央网信办发布《关于加强国家网络安全标准化工作的若干意见》
- 2016.11全国人大正式通过《网络安全法》

2017年

- 2017.06《网络安全法》正式实施
- 2017.04《个人信息和重要数据出境安全评估办法（征求意见稿）》发布
- 2017.05《网络产品和服务安全审查办法（试行）》发布
- 2017.07网信办发布《关键信息基础设施安全保护条例（征求意见稿）》

2018年

- 2018.06公安部发布《网络安全等级保护条例（征求意见稿）》
- 2018.11公安部发布《互联网安全监督检查规定》
- 2018.11公安部发布《互联网个人信息安全保护指引（征求意见稿）》

2019年

- 2019.04发布《互联网个人信息安全保护指南》
- 2019.05等级保护2.0标准正式发布
- 2019.05《网络安全审查办法（征求意见稿）》发布
- 2019.05网信办发布《数据安全管理办法（征求意见稿）》
- 2019.06网信办发布《个人信息出境安全评估办法（征求意见稿）》
- 2019.10《中华人民共和国密码法》正式通过

2020年

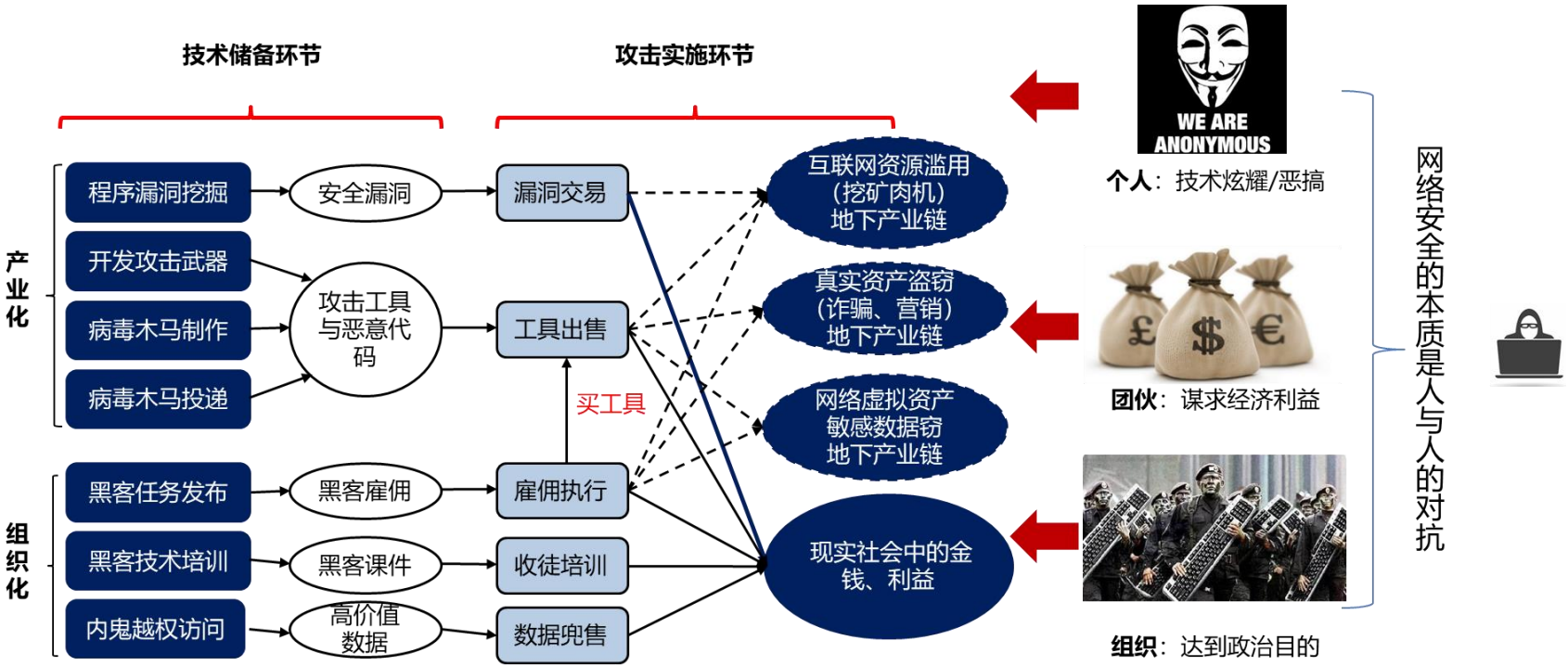
- 2020.01《密码法》正式实施
- 2020.03“七大领域”新基建进一步加快
- 2020.04十二部门联合发布《网络安全审查办法》
- 2020.07《数据安全法（草案）》征求意见稿
- 2020.10《个人信息保护法（草案）》征求意见稿

2021年

- 2021.01工信部印发《工业互联网创新发展行动计划（2021-2023年）》
- 2021.03国务院《中国十四五规划》
- 2021.08全国人大正式通过《个人信息保护法》
- 2021.09全国人大正式通过《数据安全法》

信息安全法律法规标准完善，合规要求越来越高

政策指引和实际需求



攻击呈组织化、产业化方向发展

国家、教育部、公安文保等工作要求

政策指引和实际需求

漏洞攻击

国家信息安全漏洞共享平台（CNVD）收录通用型安全漏洞13,083个，同比增长18.2%。其中，高危漏洞收录数量为3,719个（占28.4%），同比减少13.1%；“零日”漏洞收录数量为7,107个（占54.3%），同比大幅增长55.1%---**CERT 《 2021年上半年我国互联网网络安全监测数据分析报告》**

勒索病毒

尽管2021年上半年相比去年同时期，勒索病毒的攻击态势稍有下降，但勒索事件仍然频发，仅2021年第一季度，就发生了多起国际知名企业被勒索的案件，并且赎金持续刷新纪录。

----**《腾讯安全发布2020上半年勒索病毒报告》**

DDOS攻击

与2020年同期相比，2021年1月至6月的DDoS攻击总数增加了2.5倍以上。所有规模的攻击都出现了增长，最大的增长发生在规模相反的两端——100 Gbps以上的攻击增加了275%，而5 Gbps以下的非常小的攻击增加了200%以上

----**美国著名通信服务机构 Neustar公司**

网页后门

境内外8,289个IP地址对我国境内约1.4万个网站植入后门，我国境内被植入后门的网站数量较2020年上半年大幅减少62.4%。其中，有7,867个境外IP地址（占全部IP地址总数的94.9%）对境内约1.3万个网站植入后门---**CERT 《 2021年上半年我国互联网网络安全监测数据分析报告》**

外部形势依然严峻，内部威胁不可小觑

国家、教育部、公安文保等工作要求

政策指引和实际需求

北京外国语大学 BEIJING FOREIGN STUDIES UNIVERSITY

资产底数不清

多少个网站？多少个系统？
双非资产、职责范围不清

风险状态不明

漏洞、暗链、僵木蠕、数据泄露、
敏感词，预警机制？

通报流程不顺

系统归属单位？责任人？维护人？
通报给谁？

整改情况不实

是否整改？效果如何？
如何统一管控？

其他部门不配合

不整改、不配合
孤军奋战

工作成效不明显

做了哪些工作？哪些成绩？
效果如何？

网络安全管理工作的痛点

国家、教育部、公安文保等工作要求

政策指引和实际需求

北京外国语大学 BEIJING FOREIGN STUDIES UNIVERSITY

如何应对严峻的国际网络安全形势？

如何落实频发的国内安全监管要求？

如何应对常态化的重保和演练要求？

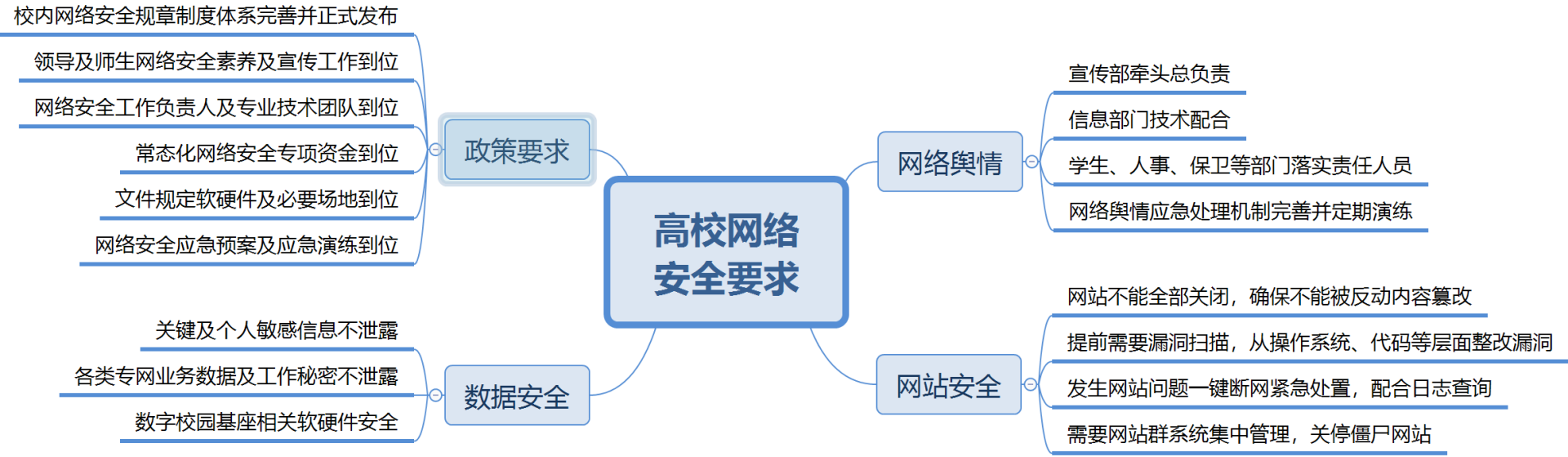
如何匹配数字化转型下的业务发展？

如何构建网络安全顶层及全局视角？

网络安全工作的思考

国家、教育部、公安文保等工作要求

政策指引和实际需求



北京外国语大学
BEIJING FOREIGN STUDIES UNIVERSITY

02

网络安全工作小结

网络安全工作小结

网信工作，人人有责！

习近平总书记指出，没有网络安全就没有国家安全，过不了互联网这一关，就过不了长期执政这一关！

领导常说“我不懂技术”，但是要懂“网络安全管理”！

有专家提出，高校推进提高治理体系和治理能力现代化，依法治校，有了信息化就是法制（好去量化和实施），没有信息化就是人治！

网络安全工作小结

一、管理到位：谁主管谁负责、谁使用谁负责

① 网络安全顶层设计到位，年度计划、五年计划

② 群防群控、层层签订《网络安全责任书》，量化风险，网络安全工作纳入部门及负责人年终考核

③ 定期召开网信领导小组工作会议，最低每个季度一次

④ 印发《十八大以来网络信息安全和网络行为管理文件汇编》等学习文件，内部管理规定正式发布，应急预案到位

⑤ 网络安全宣传周宣传，一年两次

⑥ 建立网站系统备案及年审机制，网站建设，安全第一，实用第二，美观第三

⑦ 落实整改上级通报信息系统漏洞

⑧ 定期信息系统等级保护测评整改

⑨ 年度总结汇报，定期复盘

网络安全工作小结

二、网站安全

① 学校网站统一管理，使用网站群，作为一个等保系统。

② 关停长期未更新僵尸网站，建议每月更新一条以上信息，禁止各单位在网站群外自建网站；

③ 清理禁止双非网站，限制单非网站，强制系统备案，保证服务器、域名和IP地址可管可控降低风险；

④ 网站群安全防护系统，重保时期加认证保护，仅对师生开放；

网络安全工作小结

三、信息系统安全

① 加强数据安全意识，严格数据使用流程，在一站式大厅申请使用敏感数据，需要申请报备，一事一议。泄露500条以上涉及刑责（包括行踪轨迹信息、通信内容、征信信息、财产信息等）；

② 加强数据资产意识，校内所有数据资产属于学校，推动数据公有性；

③ 升级校内人员数据编号，教职工编码升级到八位及以上；

④ 限制人脸等生物识别技术滥用。

网络安全工作小结

四、加强内部系统漏洞管理，及时处理通报漏洞。

① 定期对校内各系统进行漏洞扫描，漏洞未修复暂停校外访问；

② 加强操作系统、数据库、开放端口管理、API接口安全、小程序接口管理等；

③ 涉密系统走专网，涉密不上网，上网不涉密，需要使用国产化软硬件；

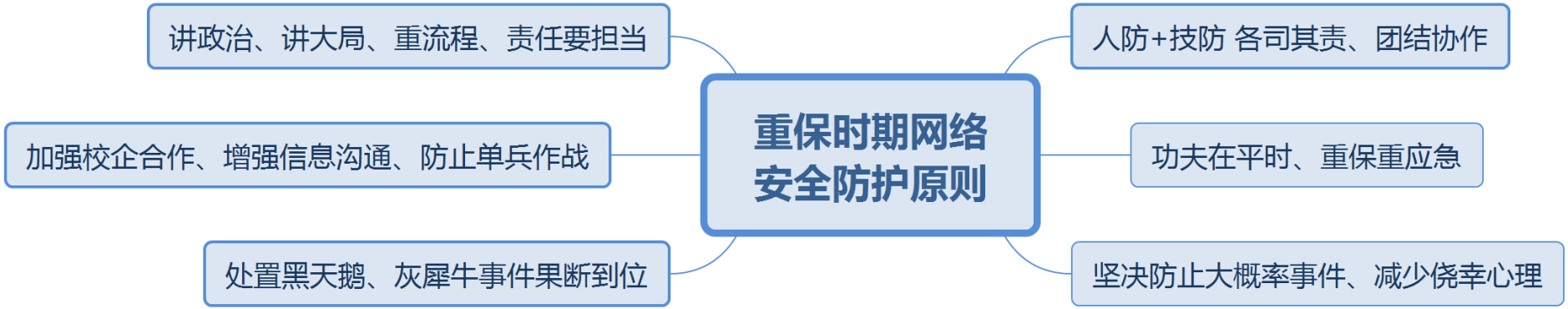
④ 校园网出口带宽加强运营商供应链管理，减少网络出口数据被劫持和分析风险。

北京外国语大学
BEIJING FOREIGN STUDIES UNIVERSITY

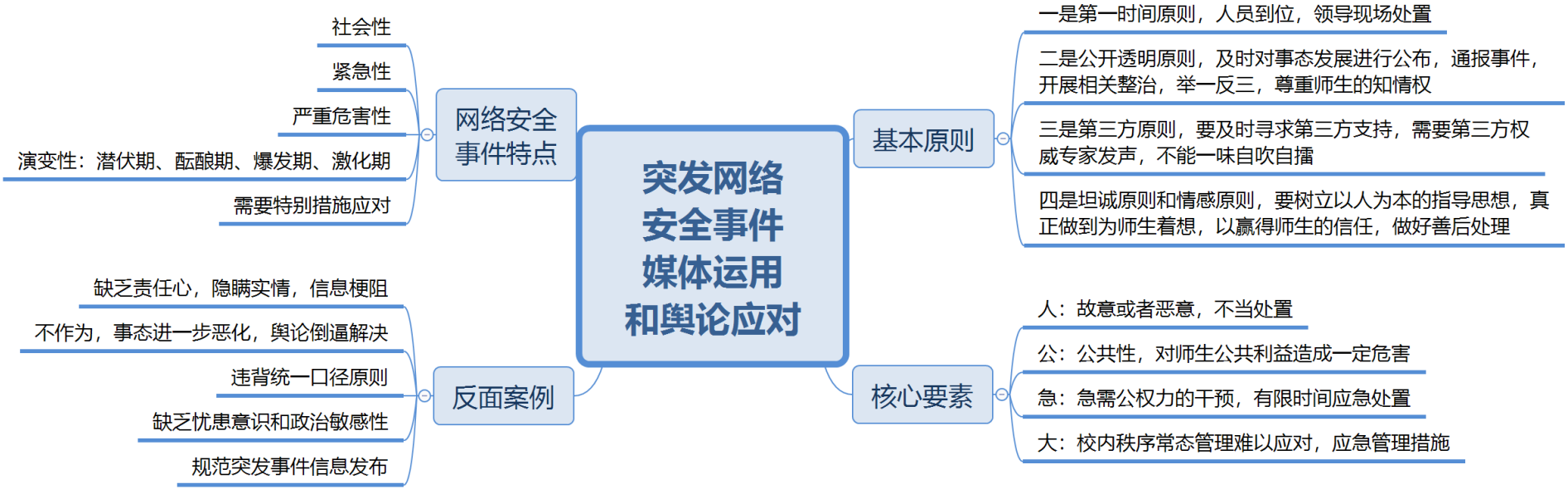
03

重保时期安全实例

重保时期安全实例


重保时期网络安全防护原则
讲政治、讲大局、重流程、责任要担当
加强校企合作、增强信息沟通、防止单兵作战
处置黑天鹅、灰犀牛事件果断到位
人防+技防 各司其责、团结协作
功夫在平时、重保重应急
坚决防止大概率事件、减少侥幸心理

重保时期安全实例


突发网络安全事件媒体运用和舆论应对
网络安全事件特点
社会性
紧急性
严重危害性
演变性：潜伏期、酝酿期、爆发期、激化期
需要特别措施应对
反面案例
缺乏责任心，隐瞒实情，信息梗阻
不作为，事态进一步恶化，舆论倒逼解决
违背统一口径原则
缺乏忧患意识和政治敏感性
规范突发事件信息发布
基本原则
一是第一时间原则，人员到位，领导现场处置
二是公开透明原则，及时对事态发展进行公布，通报事件，开展相关整治，举一反三，尊重师生的知情权
三是第三方原则，要及时寻求第三方支持，需要第三方权威专家发声，不能一味自吹自擂
四是坦诚原则和情感原则，要树立以人为本的指导思想，真正做到为师生着想，以赢得师生的信任，做好善后处理
核心要素
人：故意或者恶意，不当处置
公：公共性，对师生公共利益造成一定危害
急：急需公权力的干预，有限时间应急处置
大：校内秩序常态管理难以应对，应急管理措施

重保时期安全实例

网络安全风险一：数据机房安全

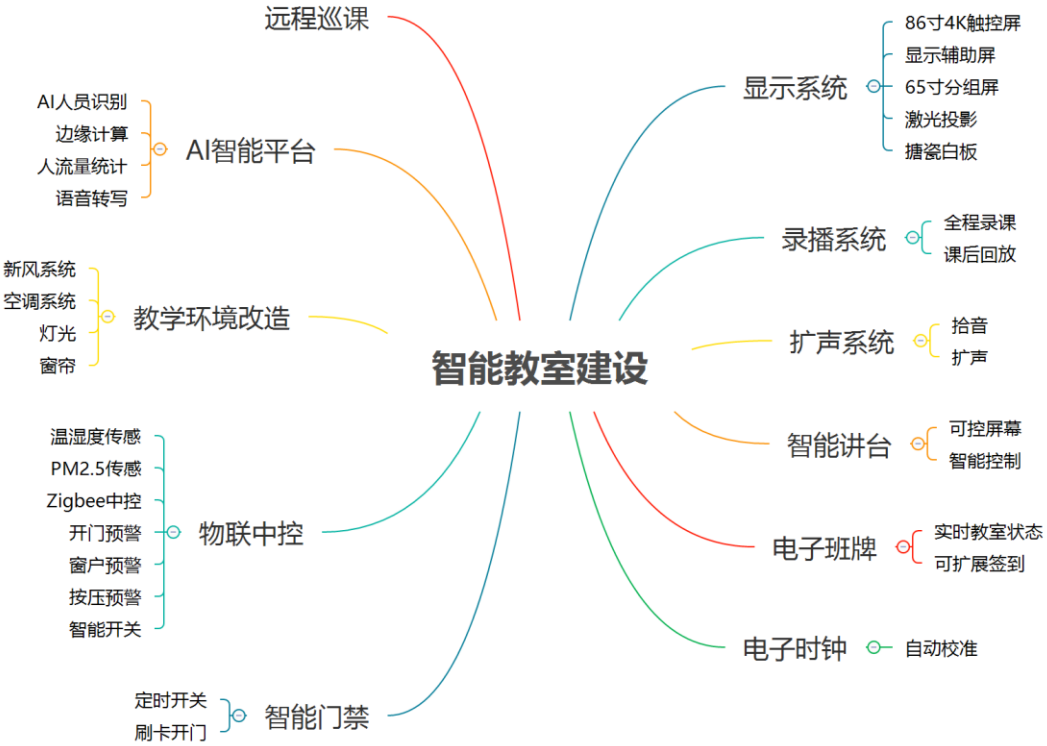
① 某学校基础数据中心机房，由于空调室外机未及时清洗、频繁停电UPS机头故障等，造成机房断电或服务器过热停止服务，引发全面断网；

② 某学校机房UPS电池漏液产生火灾，产生重大消防安全问题，造成网络舆情；

③ 某托管数据中心机房由于出口光缆被挖断，不能实事容灾备份，丢失业务数据；

④ 某高校关键存储设备故障，没有容灾和异地备份，导致所有虚拟机数据丢失，造成重大损失。

重保时期安全实例



网络安全风险二：终端安全

① 某学校传播邪教人员将非法视频拷入教师机；

② 某学校电子班牌存在外部插卡槽及控制按钮，被植入非法播放音视频；

③ 某高校教室物联网信息被攻入，物联设备被远程操控。

重保时期安全实例

网络安全风险三：硬件安全问题

① 某学校国际处办公计算机被远程控制，成为肉鸡发送大量垃圾邮件，被上级通报，原因是点击不明邮件附件导致；

② 某用户使用U盘在打印店使用过，在办公机器使用导致中招勒索病毒，造成多个数据文件无法正常使用；

③ 办公室网络摄像头被远程控制，造成个人信息泄露；

④ 部分网络用户下载不安全软件，被种植木马等程序，被黑客利用成为挖矿主机。

重保时期安全实例

网络安全风险四：个人信息泄露

① 某大学新生报考和录取信息泄露，被电话诈骗损失学费；

② 某高校教室监控视频管理不善，学生在教室不雅视频泄露，造成舆情；

③ 某高校博士报考系统被拖库，考生信息被泄露，收到大量短信和骚扰电话，涉及诈骗，影响学校声誉；

④ 公共区域接入不明wifi，存在个人信息泄露风险。

重保时期安全实例

网络安全风险五：网站安全

① 某学校网站被“反共黑客”组织攻击，贴出反动标语；

② 某单位微信号发布后台密码泄露，被别人发布无关信息，造成舆情；

③ 某学院网站存在暗链，某些引用网站域名注册失效，链接到黄赌毒网站内容；

④ 某高校二级单位一公有域名（非edu）不再使用，被别人注册打着学校名义发布无版权音视频内容，引起法律纠纷。

重保时期安全实例

网络安全风险六：数据库安全

① 某学校人员招聘网站存在任意文件上传漏洞，被攻击者上传木马后门后获得服务器权限及后台敏感数据；

② 某新闻发布网站存在SQL注入漏洞，被攻击者利用后获得大量未加密账户信息和后台敏感数据；

③ 某系统存在越权访问漏洞，可通过自行注册的低权限账号越权访问到管理员和其他用户的信息，造成敏感信息泄露问题；

④ 某学校教务系统存在暴力破解问题导致攻击者可根据学生学号规律构造脚本对学生账号进行批量爆破，获得大量学生账号和敏感信息，攻陷管理员账号后甚至更改学生成绩。

重保时期安全实例

网络安全风险七：管理和安全意识问题

① 某高校系统系统未加双因子认证保护，系统管理员电子邮件系统密码泄露，学生攻击者进入电子邮箱后，通过某关键邮件找到信息系统管理员密码，给个人上网用户进行充值；

② 某高校虚拟机管理系统后台密码比较较安全，管理员在部分虚拟机备注栏标明该应用系统等密码，但是被攻击者使用社会学攻击手段进入控制台后宣告失守，造成重大安全问题；

③ 某些网站或者淘宝店售卖各大高校图书馆资源，用户可登录网站充值或者直接购买相关账号即可访问到全国各大高校图书馆资源。

重保时期安全实例

网络安全风险八：密码和密钥安全

① 某学校无线portal认证传输密码，过程没有全程加密，被黑客探测到，盗用个人密码；

② 某学校重要系统和设备密码没有备份，设置过度复杂后无法正常进入管理系统，请厂商来恢复密码；

③ 某单位两个系统做接口，违规同步密码，机机接口和人机接口的账号未分离；读取数据库的密码项没有在创建之初进行不可逆加密，管理员用户可以轻易读取密码，导致个人密码泄露。

重保时期安全实例

网络安全风险九：专网及财务安全

① 某单位存在有线电视线路管理混乱，有人私自发布反动视频信号，触犯法律；

② 某学校财务人员不按照使用规定，在财务专网内使用个人U盘，导致专网病毒泛滥，财务系统不能正常工作；

③ 某高校一卡通使用M1卡，密钥被探测复制泄露，学生自购设备为自己卡片非法充值，部分CPU卡也在模拟M1使用；

④ 某高校校内自建视频点播系统，涉及多部未授权影视片，被校外公司取证后走司法途径，被判赔偿损失。

重保时期安全实例

网络安全风险十：供应链安全

① 前段时间的核弹级漏洞log4j2问题，应用系统依赖有严重问题的组件，爆出问题后厂商未能第一时间修复，导致0-day攻击风险极大；

② 某学校网站的开发单位由于开发人员操作不规范，将系统源代码信息公布到github平台上，造成系统源代码和重要配置文件泄露；

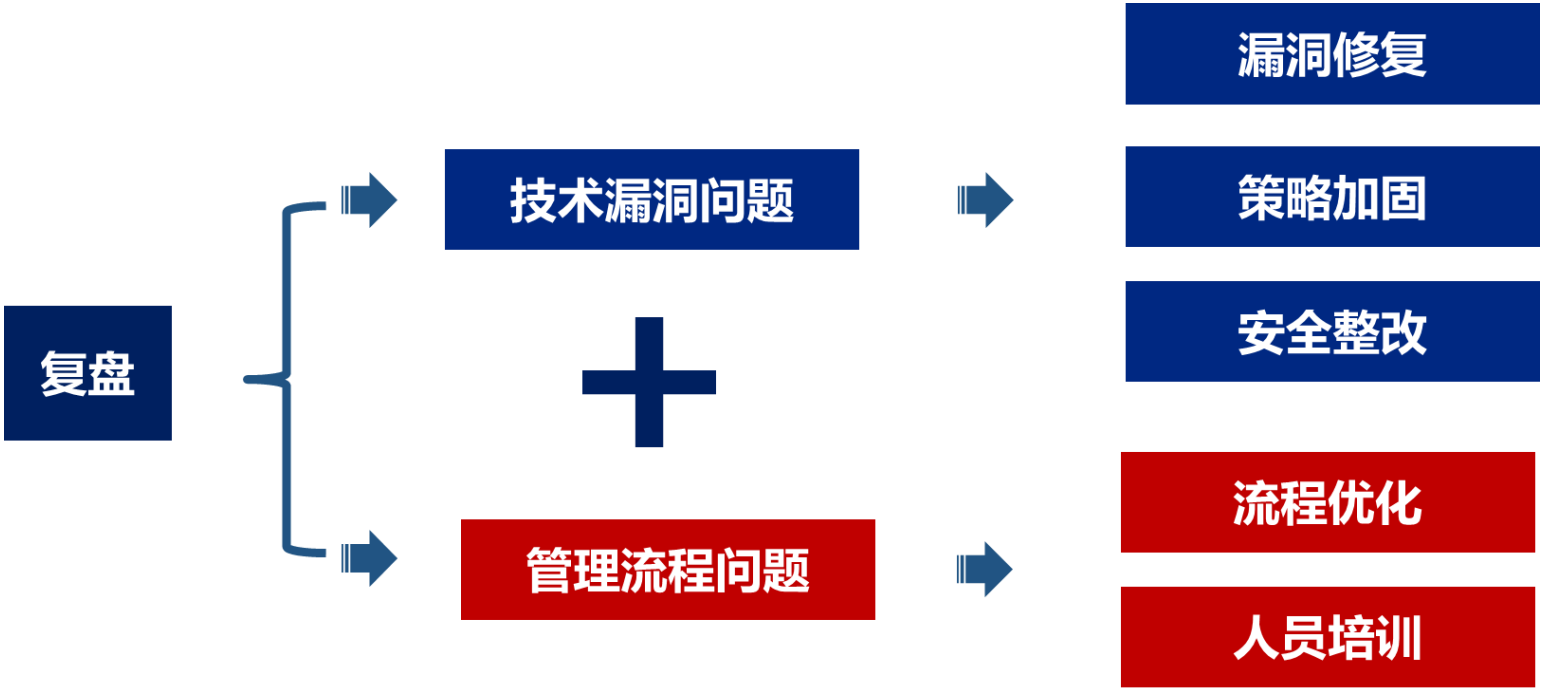
③ 某公司在进行某学校学生信息管理系统开发测试时，将大量学校师生信息存储于本公司服务器上，由于未做好防护手段导致被入侵，大量个人信息泄露。

北京外国语大学
BEIJING FOREIGN STUDIES UNIVERSITY

04

未来网络安全工作规划

未来网络安全工作规划

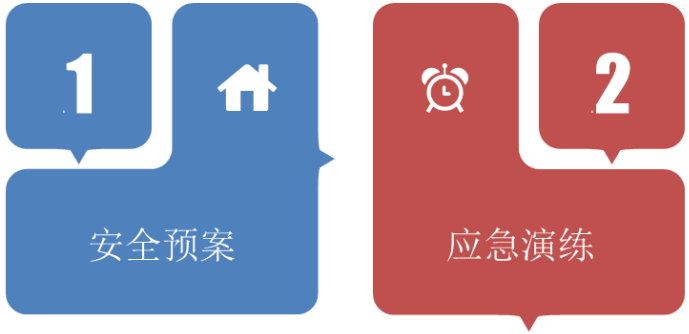


风险持续整改

未来网络安全工作规划

应急预案编制

制定分类分级的应急处置预案，建立应急处置架构，建立畅通高效沟通通道，明确应急处置处置方法，不定期开展安全审计，不断迭代优化应急预案

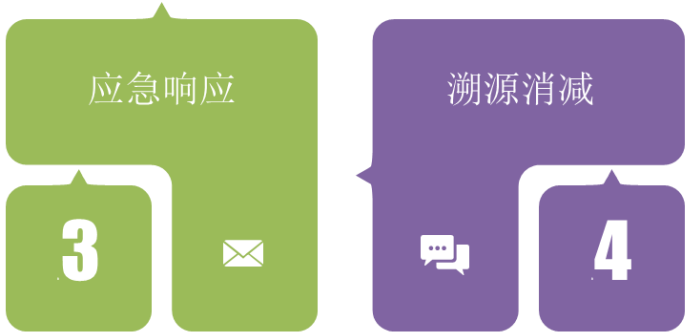


安全应急演练

根据预先设计应急演练方案，组织应急演练活动，检验应急预案的有效性，验证组织指挥能力、应急响应能力、应急处置能力和业务恢复能力

应急响应处置

在发生安全事件后，按照预案设计快速组织开展应急处置，完成问题分析、还原攻击链，定位安全漏洞，锁定攻击者及攻击手法，开展补救和反制措施，消除安全隐患，恢复业务生产



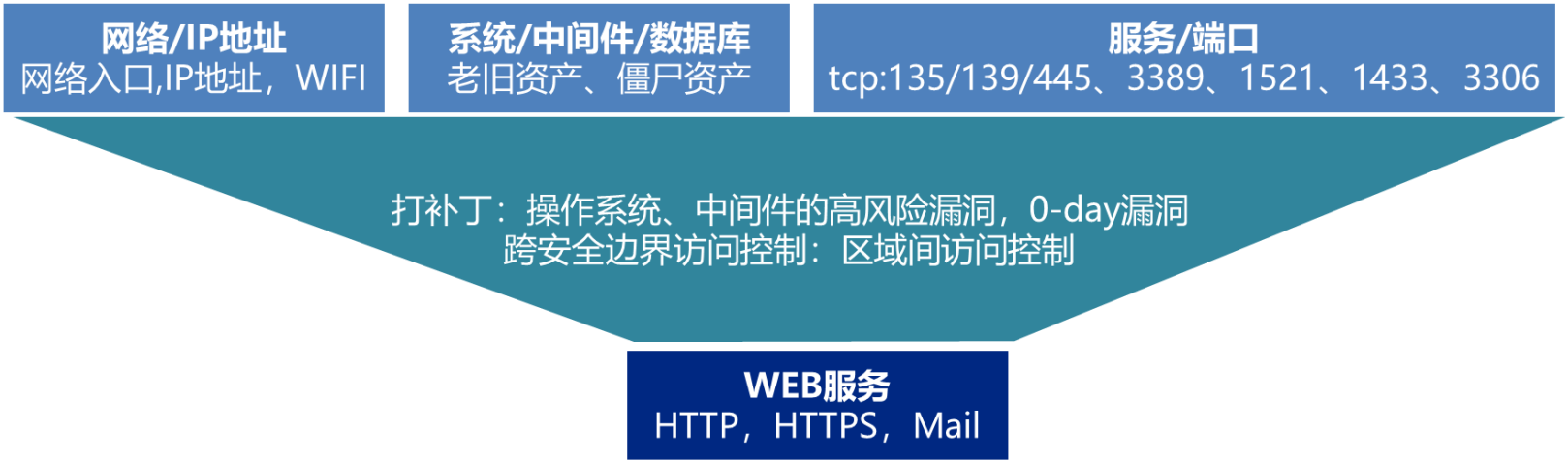
取证威胁溯源和消减

关联报文上下文还原攻击链，锁定攻击源，复原攻击手法，结合威胁情报精准绘制攻击者画像，并在法律许可的范围下开展适当的反制，迟滞网络攻击进程，为威胁处置预留时间窗口

构建应急响应体系，提升安全处置能力

未来网络安全工作规划

该关停的关停，该修补的修补，缩减互联网攻击暴露面

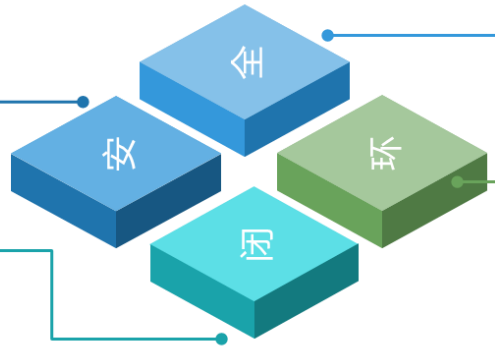


收敛互联网暴露面

未来网络安全工作规划

北京外国语大学 BEIJING FOREIGN STUDIES UNIVERSITY

常态化安全运营



绘制资产图谱，清理资产风险

定期性资产稽查，探测资产指纹，摸清资产家底，清理风险资产，减少资产互联网暴露面，对资产进行全生命周期监管

基于风险分级的漏洞闭环管理

全方位探测资产安全风险，根据资产重要级别定制不同的漏洞深度扫描策略，根据漏洞风险级别重新定期漏洞修复优先级，有序推进漏洞管理闭环

借助云端威胁情报实现联防联控

利用安全大数据分析技术，深度感知网络安全威胁，结合威胁情报快速研判，降低告警误报率和漏报率，快速响应和处置，对威胁持续跟踪，实现威胁管理闭环

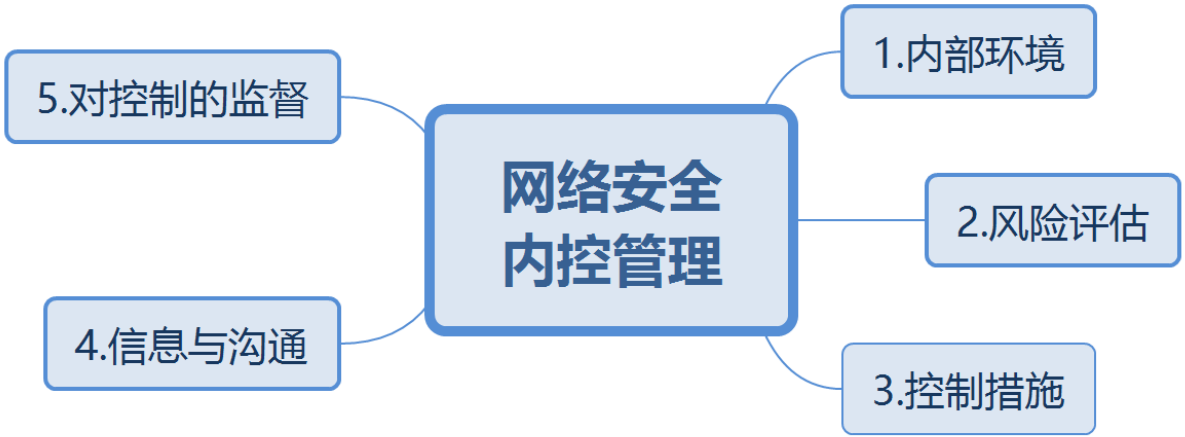
全事件类型监测，快速响应处置

7*24小时对全类型安全事件进行监测。当发生事件时，按标准事件流程，及时启动事件响应，评估事件影响，有序推进事件的处置，及时止损、快速溯源、消除影响，恢复生产，对事件的全过程进行跟踪和管理

最终目标：实现资产、漏洞、威胁、事件闭环管理

未来网络安全工作规划

从网络安全目标出发，到安全控制措施的落地实施，
实施网络安全内控管理



COSO模型、SXO模型、COCO框架等

未来网络安全工作规划

开放　互联　智能　融合　创新

北京外国语大学
BEIJING FOREIGN STUDIES UNIVERSITY

英语并置 博客篇行

谢 谢！