2021年首届川渝高校教育信息化峰会

聚焦十四五 · 展望新时代

“十四五”时期
高校网络安全保障体系和能力建设探索

主讲：李卫东

东华理工大学信息办、网络与信息中心 副主任

江西教育网络安全应急中心、江西省网络空间安全实训基地 副主任

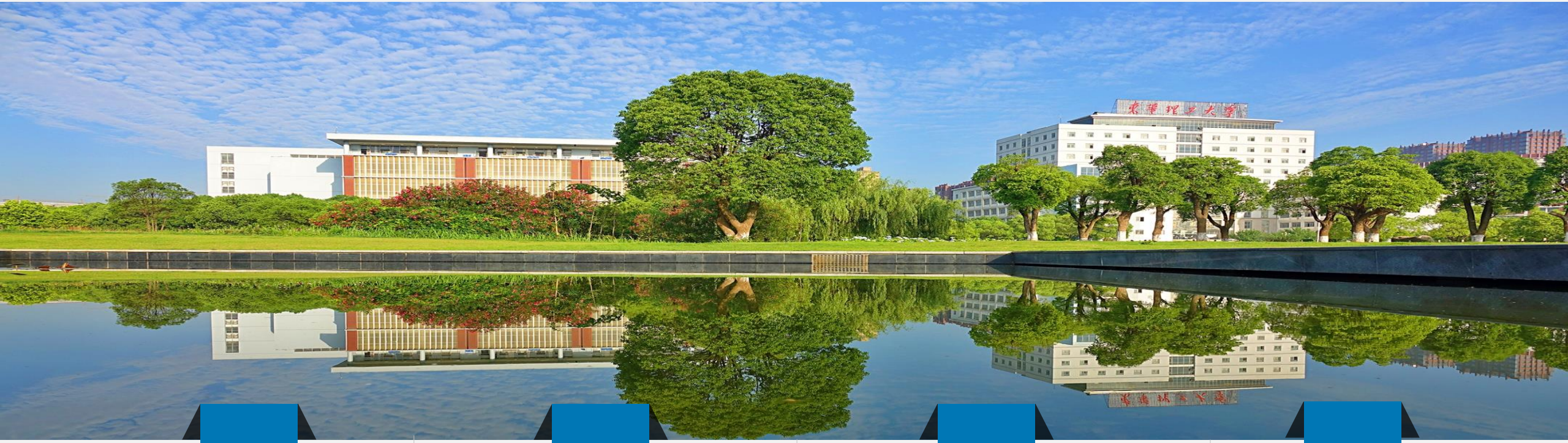
江西省互联网信息学会 副秘书长

東華理工大學
EAST CHINA UNIVERSITY OF TECHNOLOGY

原华东地质学院，隶属于核工业部，中国核工业第一所高等学校，1956年建校，江西省人民政府与国家国防科技工业局、自然资源部、中国核工业集团公司共建，具有核地学和核科学特色的综合性大学。目前在校本、硕、博学生3万余人，建有江西南昌和抚州两个校区。

为核成立、因核成名、以核成势

CONTENT



/01 “十三五”建设成效与问题

网信基础设施建设取得新进展

互联网出口链路 4 条，IPv4/v6总带宽 55 G，ONU光终端 9000+ 个，光缆线路 4000+ 条，总长度 40+ 公里，上网用户数量 3.5 万，数据中心 2 个，网络机柜 100+，物理服务器 100+ 台，虚拟机 300+ 个

模块化数据中心

超融合私有云平台

智慧校园应用建设取得新成效

从数字化校园到智慧校园的迭代升级，各类网站 100+ 个，公共服务平台、业务信息系统 50+ 个，面向师生网上办事服务 6 大类、100+ 项

统一身份认证平台

一站式网上办事服务大厅

让数据多跑路，让师生少跑腿

网信体制机制建设取得新突破

校园网络安全和信息化工作领导小组

挂靠网络与信息中心
书记、校长双组长

2014年

2017年

信息化建设与管理办公室

（网络与信息中心合署）
江西教育网络安全工作小组
《东华理工大学信息化建设管理办法（试行）》

江西省教育专网骨干节点单位

江西高校教育信息化学会网络安全专委会
《东华理工大学网络安全应急预案》

2018年

2019

江西教育网络安全应急中心

网络安全预警通报、应急处置
“国家网络安全宣传周”校园日
高校网络安全技能竞赛

江西省网络空间安全实训基地

联合成立网络空间安全学院
网络安全工作责任制考核

2020

2021

江西省网络空间安全与应急技术重点实验室（筹）

网络安全保障与应急技术
应用与研究

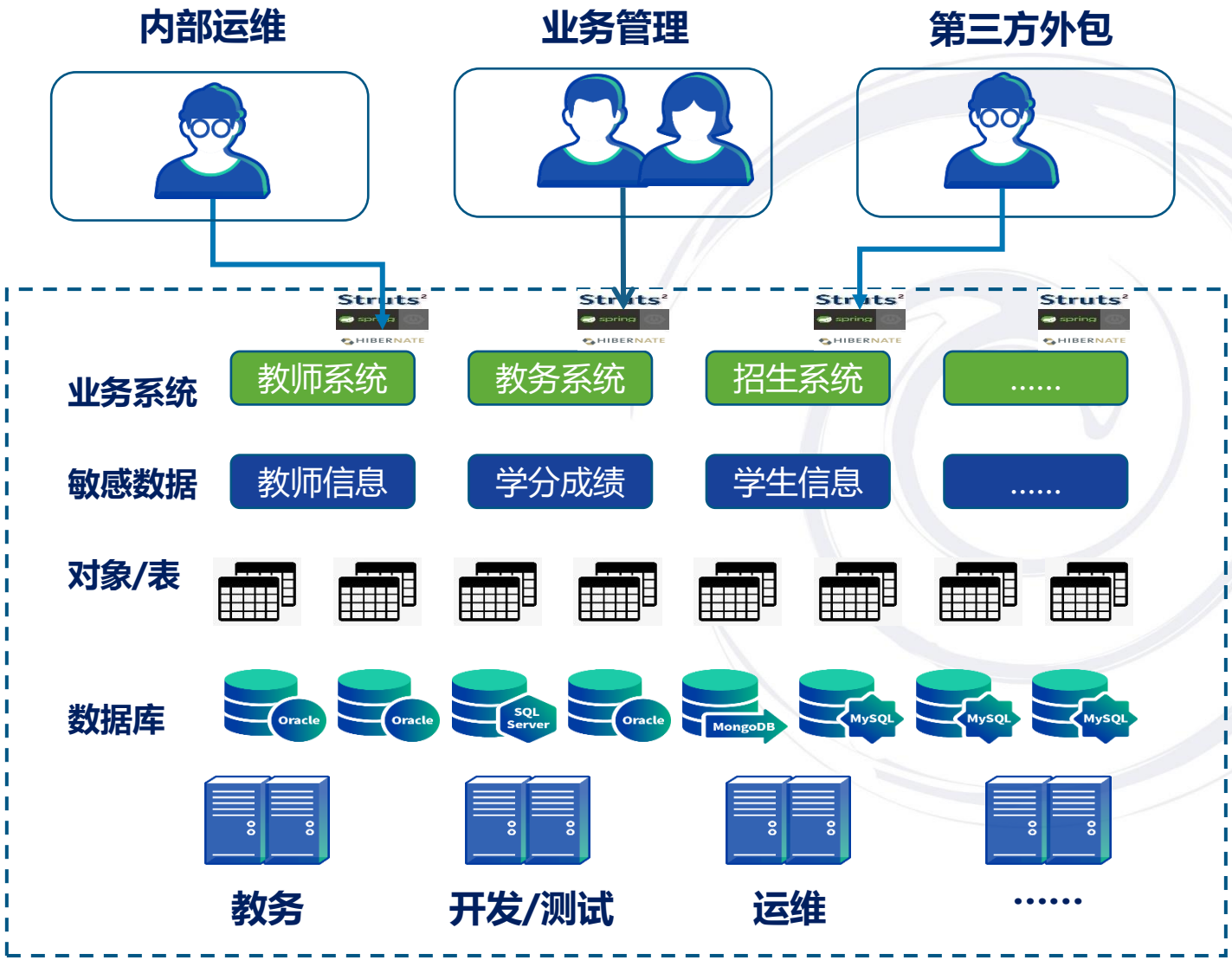
网络安全能力建设取得新提升

构建校级网络安全态势感知平台和运维监控中心，落实网络安全等级保护制度，开展二级单位网络安全责任制考核，推动网络安全“三同步”建设

网络安全态势感知平台

网络安全运维监控中心

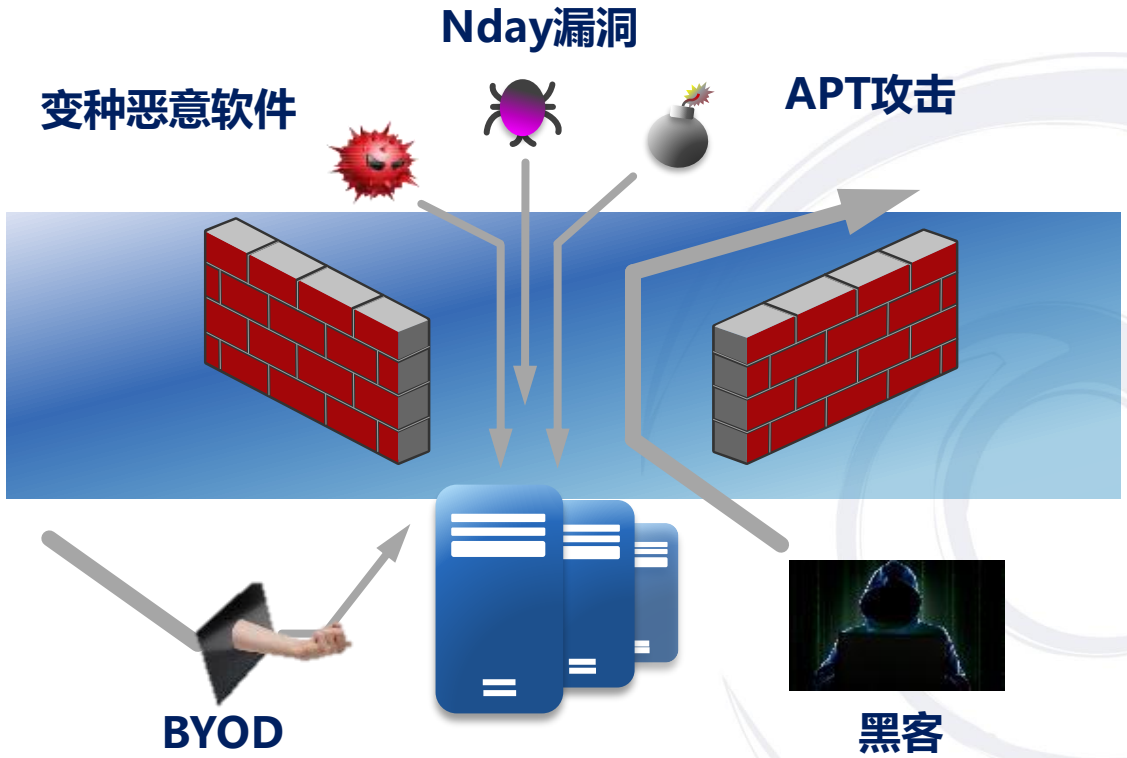
困难和挑战-1：网信资产底数不清，无法细化责任边界



高校网信资产现状分析

- 不知道网络有多少资产（业务系统、中间件、数据库、虚机、服务器、网络设备、IP、端口等）；
- 二级学院多，资产频繁的上线、下线，存在大量影子资产、废弃资产，给黑客留下大量机会；
- 缺乏精细化的资产管理手段，导致安全措施无法落到实处。

困难和挑战-2：技术对抗力量不强，无法预知安全威胁



- 网络安全人才队伍力量薄弱，防护对抗能力不足
- 高校用户多、系统多，暴露面过多，漏洞多，修复困难
- 传统杀病毒、防火墙、入侵检测“老三样”已经难以应对网络外部攻击
- 防护边界模糊，端口映射混乱；网络区域划分不合理，未按照业务等级划分
- 针对云、大、物、移等新技术，缺乏有效安全防护措施

网络黑链

网络电诈

勒索病毒


数据泄露

困难和挑战-3：应急响应能力不足，无法清零安全事件

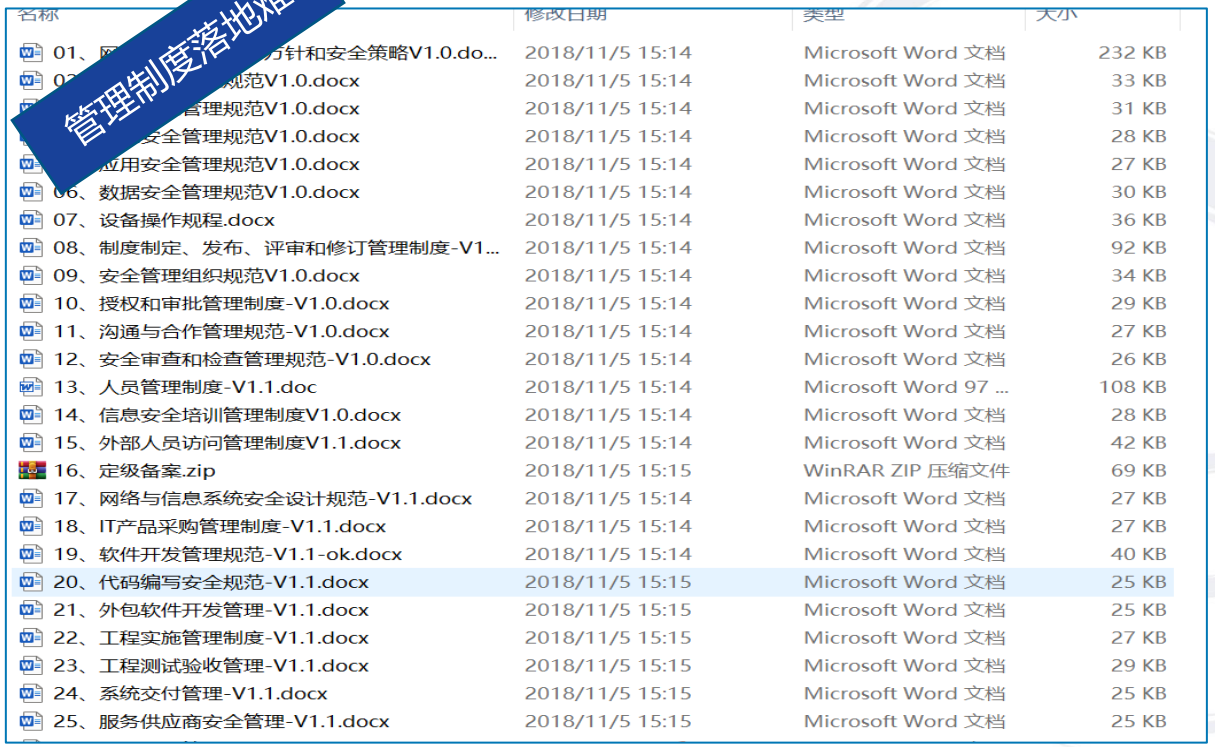
漏洞通报处置困难

时间		等级	作者
	存在SQL注入漏洞	高危	吾鑫
	存在弱口令	中危	0verWatch
2020-06-13	存在其他漏洞	中危	JunMo
2020-06-13	存在其他漏洞	高危	JunMo
2020-06-13	.学院存在弱口令	高危	main2
2020-06-13	技术学院存在弱口令	高危	main2
2020-06-13	在SQL注入漏洞	中危	applicantA...
2020-06-13	存在弱口令	中危	vul_chang
2020-06-13	存在SQL注入漏洞	中危	default
2020-06-13	在SQL注入漏洞	中危	default
2020-06-13	存在SQL注入漏洞	中危	default
2020-06-13	存在文件上传漏洞	高危	0verflow
2020-06-13	存在SQL注入漏洞	中危	default
2020-06-13	存在弱口令	中危	chaser
2020-06-13	存在SQL注入漏洞	中危	default

- 重设备投入、轻后期运维
- 大量网络安全事件需要手工干涉处理，设备无法联动处置
- 无运营支撑流程、工具，发生安全事件时，没有能力进行闭环处置，被动响应处置时间过长

困难和挑战-4：安全保障体系不全，无法落实安全责任

管理制度落地难



名称	修改日期	类型	大小
01、网[illegible]方针和安全策略V1.0.do...	2018/11/5 15:14	Microsoft Word 文档	232 KB
02[illegible]规范V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	33 KB
[illegible]管理规范V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	31 KB
[illegible]安全管理规范V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	28 KB
[illegible]应用安全管理规范V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	27 KB
06、数据安全管理规范V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	30 KB
07、设备操作规程.docx	2018/11/5 15:14	Microsoft Word 文档	36 KB
08、制度制定、发布、评审和修订管理制度-V1...	2018/11/5 15:14	Microsoft Word 文档	92 KB
09、安全管理组织规范V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	34 KB
10、授权和审批管理制度-V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	29 KB
11、沟通与合作管理规范-V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	27 KB
12、安全审查和检查管理规范-V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	26 KB
13、人员管理制度-V1.1.doc	2018/11/5 15:14	Microsoft Word 97 ...	108 KB
14、信息安全培训管理制度V1.0.docx	2018/11/5 15:14	Microsoft Word 文档	28 KB
15、外部人员访问管理制度V1.1.docx	2018/11/5 15:14	Microsoft Word 文档	42 KB
16、定级备案.zip	2018/11/5 15:15	WinRAR ZIP 压缩文件	69 KB
17、网络与信息系统安全设计规范-V1.1.docx	2018/11/5 15:14	Microsoft Word 文档	27 KB
18、IT产品采购管理制度-V1.1.docx	2018/11/5 15:14	Microsoft Word 文档	27 KB
19、软件开发管理规范-V1.1-ok.docx	2018/11/5 15:14	Microsoft Word 文档	40 KB
20、代码编写安全规范-V1.1.docx	2018/11/5 15:15	Microsoft Word 文档	25 KB
21、外包软件开发管理-V1.1.docx	2018/11/5 15:15	Microsoft Word 文档	25 KB
22、工程实施管理制度-V1.1.docx	2018/11/5 15:15	Microsoft Word 文档	27 KB
23、工程测试验收管理-V1.1.docx	2018/11/5 15:15	Microsoft Word 文档	29 KB
24、系统交付管理-V1.1.docx	2018/11/5 15:15	Microsoft Word 文档	25 KB
25、服务供应商安全管理-V1.1.docx	2018/11/5 15:15	Microsoft Word 文档	25 KB

三分技术，七分管理

- 制度体系不健全，缺乏规范、指南、流程、表单做支撑，与实际情况不符；
- 针对云、大、移、物等新技术新业务，未建立相关安全管理办法、规范；
- 专职网络安全队伍人员编制少，二级单位兼职管理员人少、不稳定；
- 二级单位网络安全意识不强，管理责任分工不明确，考核评价机制不健全

/02 “十四五”网络安全发展态势

国家推动构建网络空间命运共同体

十四五规划和2035远景目标

第十八章 营造良好数字生态 第三节 加强网络安全保护
第四节 推动构建网络空间命运共同体

信息化	互联网	网络空间	网络安全
Informationize	Internet	Cyberspace	Network Security
09 次	12 次	04 次	14 次

2021年两会政府工作报告

加强网络安全、数据安全和个人信息保护

国家出台数据安全法，保障数据安全

中华人民共和国
数据安全法

含草案说明

第一章	第二章	第三章	第四章	第五章	第六章	第七章
总则	数据安全与发展	数据安全制度	数据安全保护义务	政务数据安全与开放	法律责任	附则

2021年6月10十三届全国人民代表大会常务委员会第二十九次会议正式通过，9月1日开始施行
中华人民共和国数据安全法全文共 7 章 55 条 5300 余字

教育部部署新时代教育管理信息化工作

17. 提升安全保障能力

- 落实《网络安全法》等法律法规和政策要求，**建立健全网络安全责任体系**
- 落实网络安全等级保护制度，重点保障**关键信息基础设施**
- 开展网络安全监测预警通报，提升**网络安全态势感知能力**
- 建立**供应链安全管理体系**，定期组织审计，国产化
- 加强**数据安全保障**，重点保护师生和家长个人隐私信息

中华人民共和国教育部

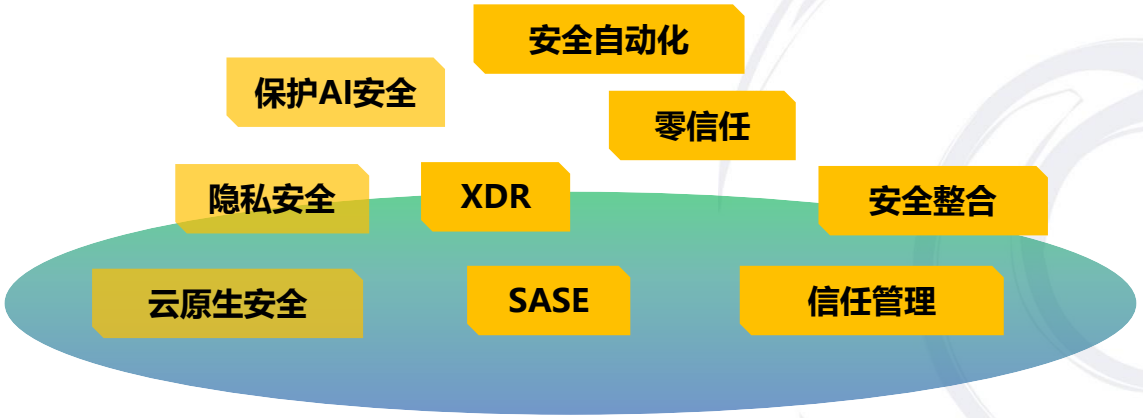
教科信函〔2021〕13号

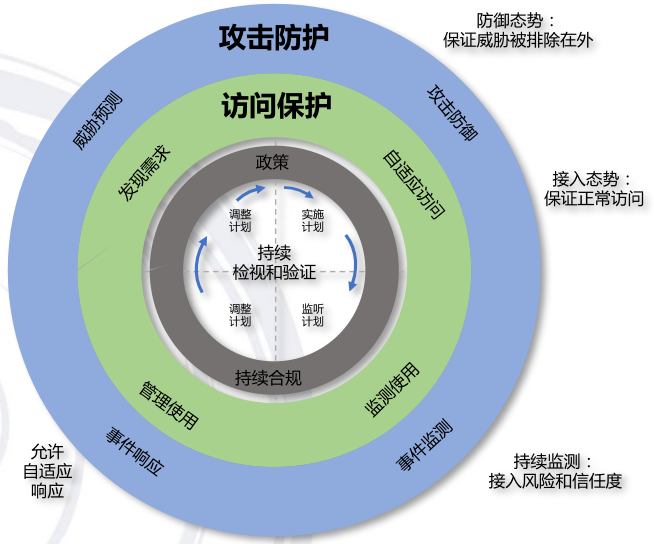
教育部关于加强新时代教育管理信息化工作的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，部属各高等学校、部省合建各高等学校，各直属单位：

国内外网络安全技术发展的最新趋势

聚焦业务数据　自动化应对威胁　管理信任　整合落地





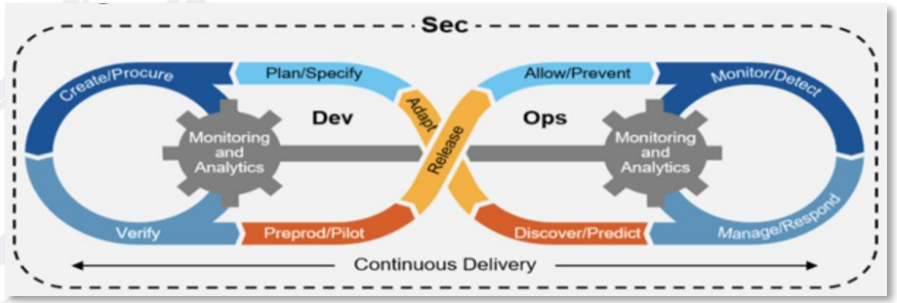
持续自适应风险与信任评估

CARTA

- 攻击防护与访问保护
- 自适应闭环
- 数据驱动的持续监测和评估

Gartner 2020九大安全与风险趋势

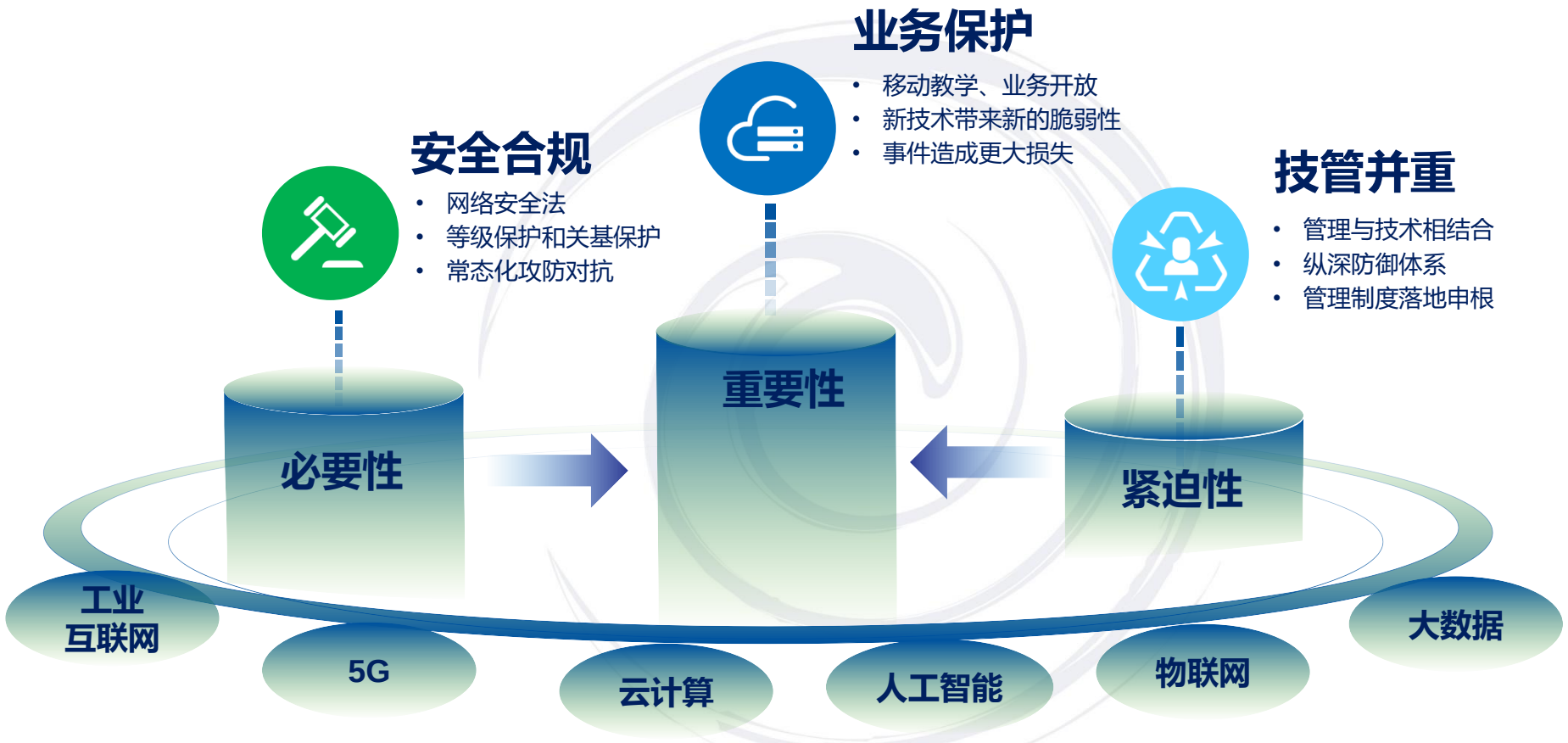
- 人员短缺、云计算快速迁移、法规遵从、威胁快速演变，仍然是当前最重要的主要安全挑战
- 新冠疫情影响下，组织机构更加关注基于云实现的安全和操作，远程访问策略和工具，迁移到云和采用SaaS应用程序



安全与业务的融合

- 业务创建阶段的保护
- 向业务提供安全的导轨，而不是门

新基建背景下高校网络安全建设新需求



新型基础设施建设，网络安全建设以“业务数据保护”为中心

做好新时期网络安全规划的五个转变

01 从局部整改到全面综合能力建设

02 从数据资源到数字教育安全保障

03 从重要系统保护到关基领域保护

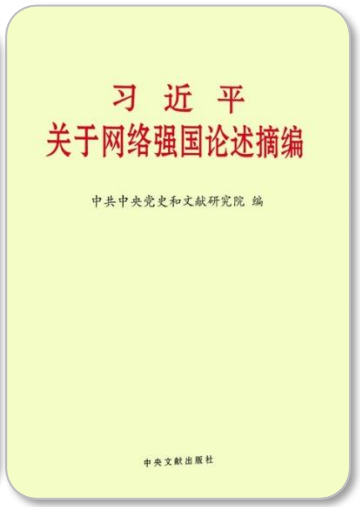
04 从专业到学科建设培育安全人才

05 从基础保障到网络空间综合治理

/03

新时期网络安全体系规划建设

根本遵循：习近平关于网络强国的重要论述



党的十八大以来，习近平总书记高度重视网络安全和信息化工作，从信息化发展大势和国际国内大局出发，就网信工作提出了一系列新思想新观点新论断，深刻回答了一系列方向性、根本性、全局性、战略性重大问题，形成了内涵丰富、科学系统的**习近平总书记关于网络强国的重要思想**，为做好新时代网络安全和信息化工作指明了**前进方向**、提供了**根本遵循**。

总体目标：构建网络安全综合保障体系

东华理工大学
网络安全保障体系

以能够抵御国家级组织的攻击能力为 **标尺**

以等级保护2.0、关键信息基础设施防护要求为 **指导**

以数据不被批量泄露、网页不被篡改、平台不被破坏为 **底线**

以国产密码、自主可控技术为 **支撑**

以涵盖安全管理、态势感知、安全服务等维度的安全运营平台为 **中心**

以智能、防护、检测和响应（应急处置）为 **主线**

顶层设计：“技术+管理+运营+保障”四位一体

重点任务-1：网络安全等级保护2.0合规工程

网络安全等级保护2.0技术框架体系

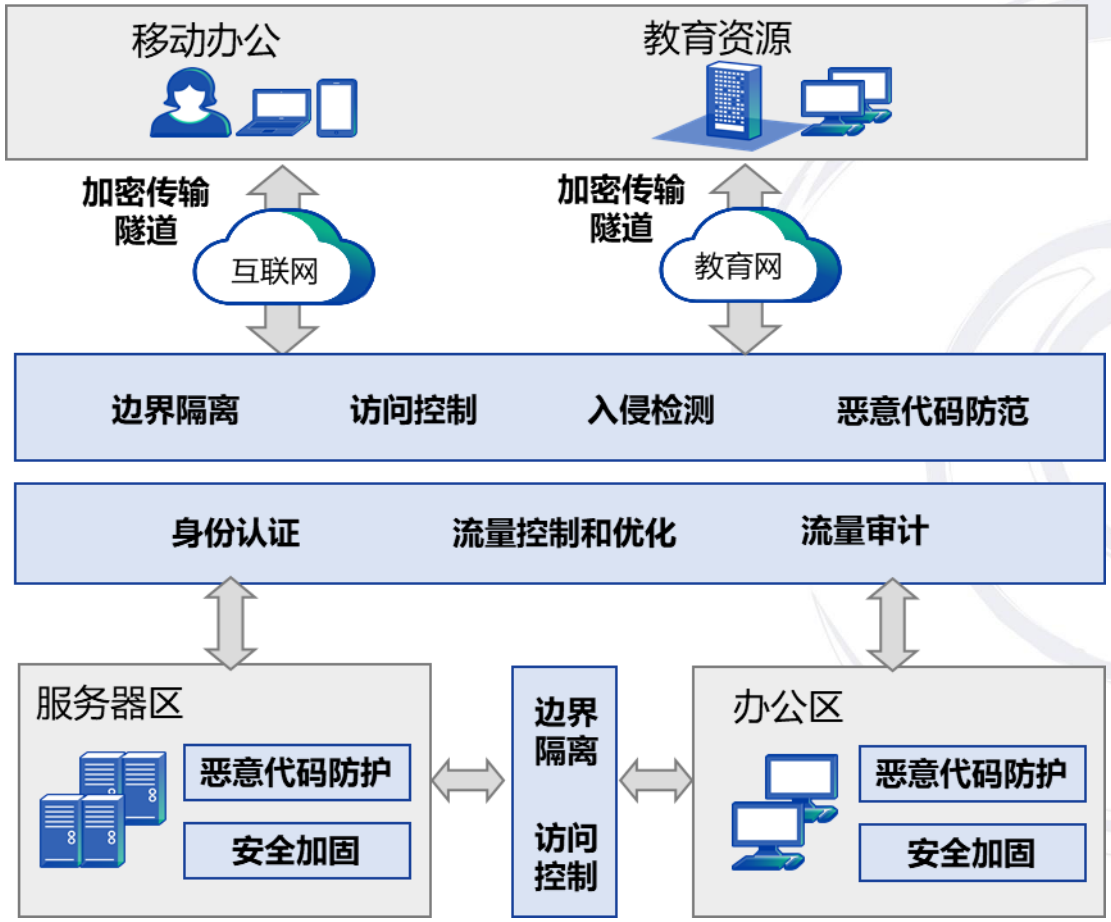
防护框架：

- 以**“一个中心”**管理下的**“三重防护”**体系框架，构建整体安全防护体系；
- 最终做到**整体防御、分区隔离**；**积极防护、内外兼防**；**自身防御、主动免疫**；**纵深防御、技管并重**。

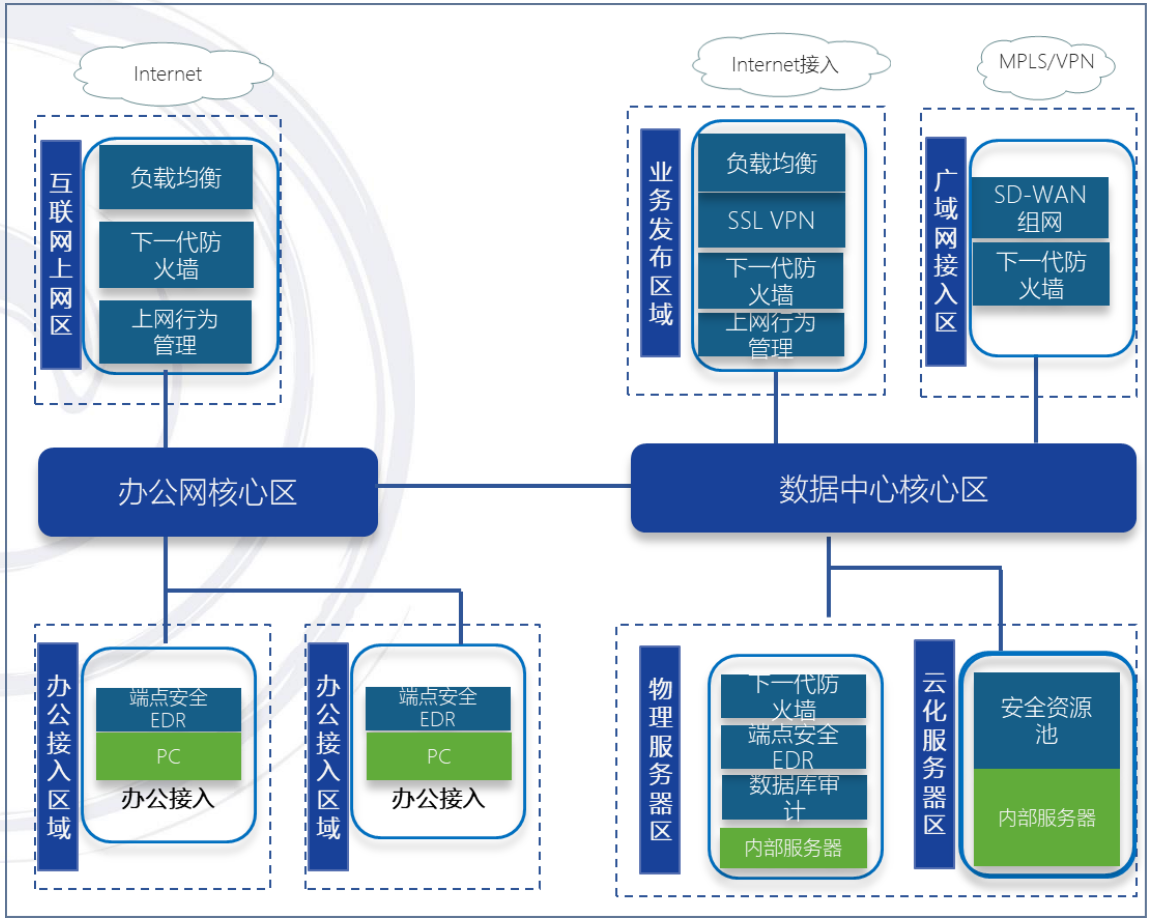
目标要求：

- 对于传统威胁，要做到**快速、精准防护**；
- 对于新型网络攻击，要做到**智能检测与分析**；
- 建设**“可视、可控、可管、可追溯”**的网络安全治理能力；
- **感知校园网络安全态势**；
- 规范数据处理活动，**保障教育数据安全**

重点任务-2：纵深、主动防御体系构建工程



网络基础设施安全防护加固



区域边界隔离与安全防护

重点任务-2：纵深、主动防御体系构建工程

被动防御

防御为主、被动响应

- 边界隔离
- 入侵防护
- 主机杀毒

缩小攻击面，提升攻击成本

主动防御

持续监测、快速响应

- 持续监测
- 智能分析
- 协同联动

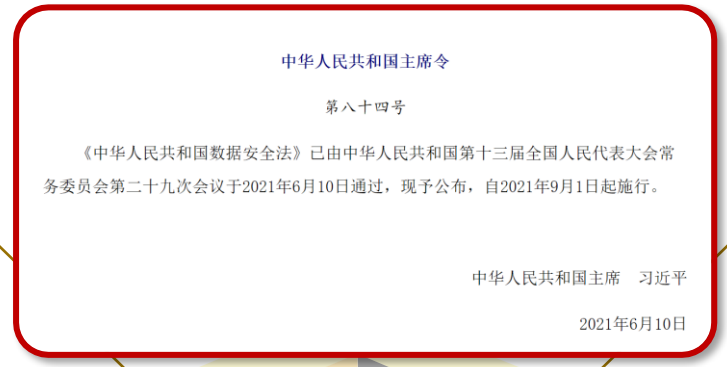
提早发现，缩短检测和响应时间

构建防御、检测、响应于一体的主动防御体系，重点关注持续监测、快速响应能力建设

重点任务-3：数据治理与数据安全保障工程

意识宣贯

- 桌面屏保
- 意识培训
- 微信推送
- 安全周



中华人民共和国主席令

第八十四号

《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过，现予公布，自2021年9月1日起施行。

中华人民共和国主席　习近平

2021年6月10日

数据安全管理类保护措施

- 数据安全管理组织架构及职责分配
- 数据安全整体管理策略
- 数据安全分类分级标准
- 数据安全事件应急响应流程
- ……

数据安全技术防护措施

- 网络及应用层DLP
- 终端桌面管控
- 邮件DLP
- 统一身份认证系统（堡垒机）
- 数据库操作审计系统
- ……

技术测试

- 钓鱼测试
- 渗透测试
- 漏洞扫描
- 基线核查

数据安全目标

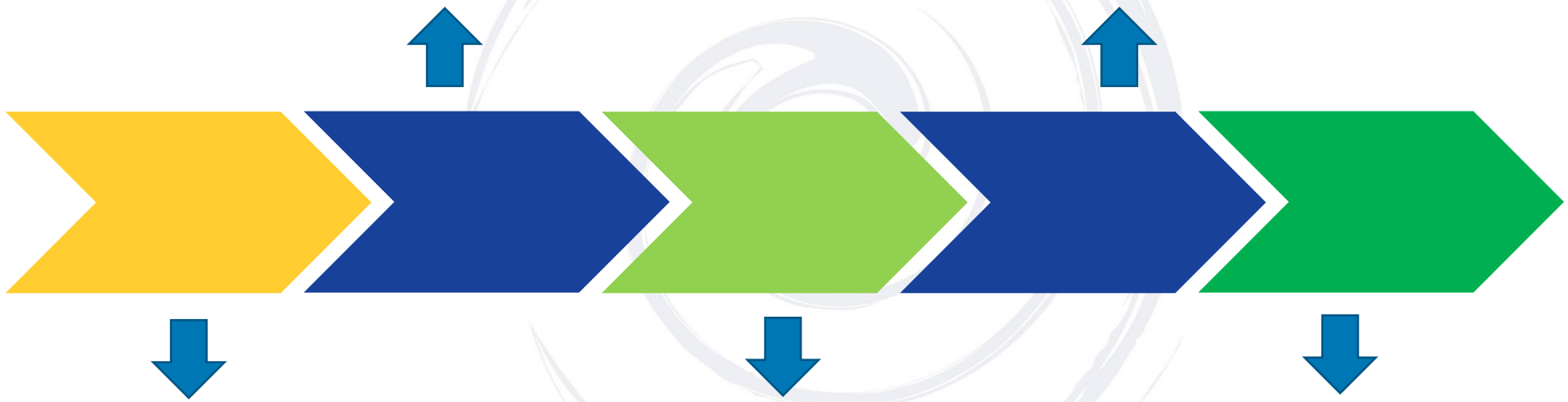
持续开展数据安全风险检查，验证管理类措施以及技术类措施的有效性.

基于差距分析和风险评估的结果，全面梳理数据资产面临的安全风险，形成整体数据安全体系规划（管理和技术）

重点任务-4：网络安全管理流程再造工程

工作流程一张表：构建基于业务系统全生命周期的安全运维流程，明确相关责任及权限

安全风险一张表：以业务资产、PC终端、基础网络三个维度，形成漏洞、威胁及安全事件的统一视图



业务资产一张表：业务资产名称、IP地址、责任人、联系方式、操作系统、数据库、端口及服务开放情况等

管理制度一张表：围绕业务系统、数据、其他IT资产生命周期安全，梳理出管理制度

平战结合一张表：分为平时（急时）、战时，将工作安排好，月主题，如漏洞处置、安全基线等

重点任务-5：全流程闭环安全运营体系建设工程

运营管理层（云端）

运营管理层（本地）

安全设备层

安全运营

运维人员　安全厂商

工单触发　工单处置　反馈建议

事件分析、上报

触发人工服务

安全集中管理

设备监控　策略联动　告警推送　订阅服务

安全态势感知

攻击流量分析　病毒木马事件　UEBA行为分析　事件追溯

设备的集中管控

采集资产、威胁数据

边界网关：
下一代防火墙
上网行为管理
入侵威胁检测

硬件边界安全网关

流量探针检测：
采集流量、感知资产、漏洞变化

日志采集器
采集交换机、防火墙等日志

采集器

超融合云数据中心

终端桌面云

业务+终端规划

运营保障机制

运营组织

运维流程

日常运维机制

应急响应机制

规章制度

重点任务-6：师生安全意识和技能素养提升工程




安全意识培训	安全攻防渗透培训	安全认证培训	安全战略规划培训
培训对象：全校师生 **目标：**在日常生活、学习、工作中能够具备个人网络安全意识	**培训对象：网信部门教师及二级单位网络安全员** **目标：**能够处理并分析威胁，执行紧急与例行漏洞扫描任务；具备进行攻防演练能力	**培训对象：网信部门教师** **目标：**具备体系化安全建设能力，能够理解和落地网络安全法等级保护相关标准及要求	**培训对象：网信部门教师** **目标：**具备制定整体安全策略安全目标安全规划建设能力

实施计划：统筹推进、分步实施

2021-2022

第一阶段：基础防护及安全运营落地

1.基于等保2.0进一步划分好安全域，加强纵深防护；
2.加强边界和端点安全建设，具备基本的安全防护能力；
3.构建安全运营中心、通报预警能力以及安全运营管理制度；

目标：构建安全运营管理体系打下基本功

实施范围：数据中心安全、网络边界安全

2022-2023

第二阶段：内外部防护能力提升

1.围绕数据生命周期开展安全建设；
2.基于云网端进一步加外部威胁防护；
3.基于ISO27001完善信息安全管理制度
4.其他合规内容建设。

目标：重点突破 完善风险治理

实施范围：数据安全为主、整体安全

2024-2025

第三阶段：基于风险初步自适应安全

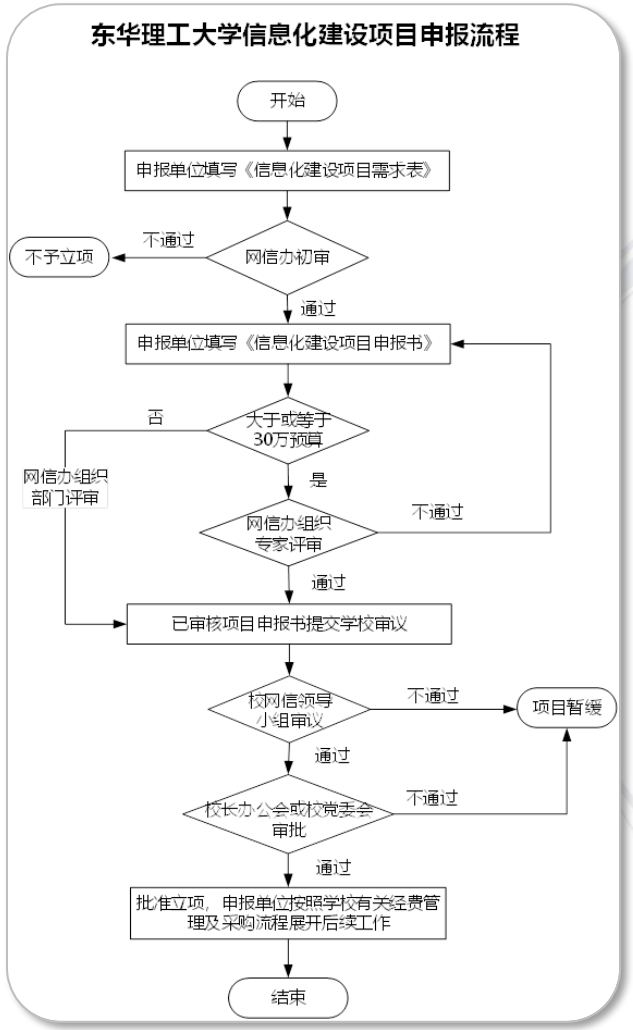
1.加强安全运营管理，全面补齐人员、制度、流程、工具第四短板
2.安全运维支撑平台建设。加强IT运维、故障排除、业务性能监测方面的建设。
3.全局安全运营，安全编排和自适应响应，零信任身份和权限管理

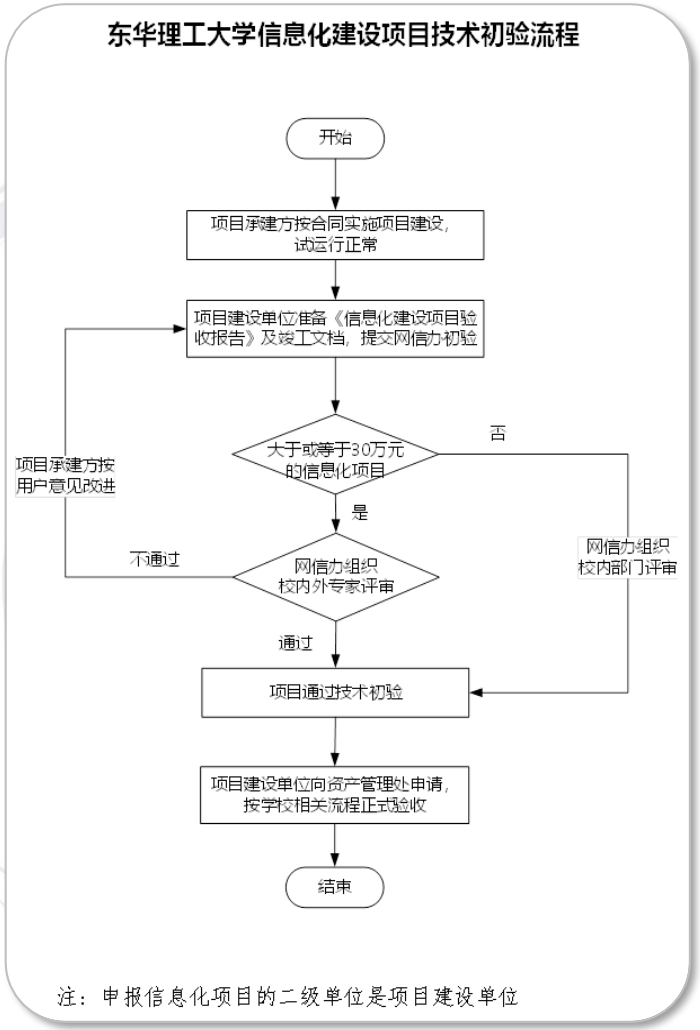
目标：基于风险形成主动化防御机制

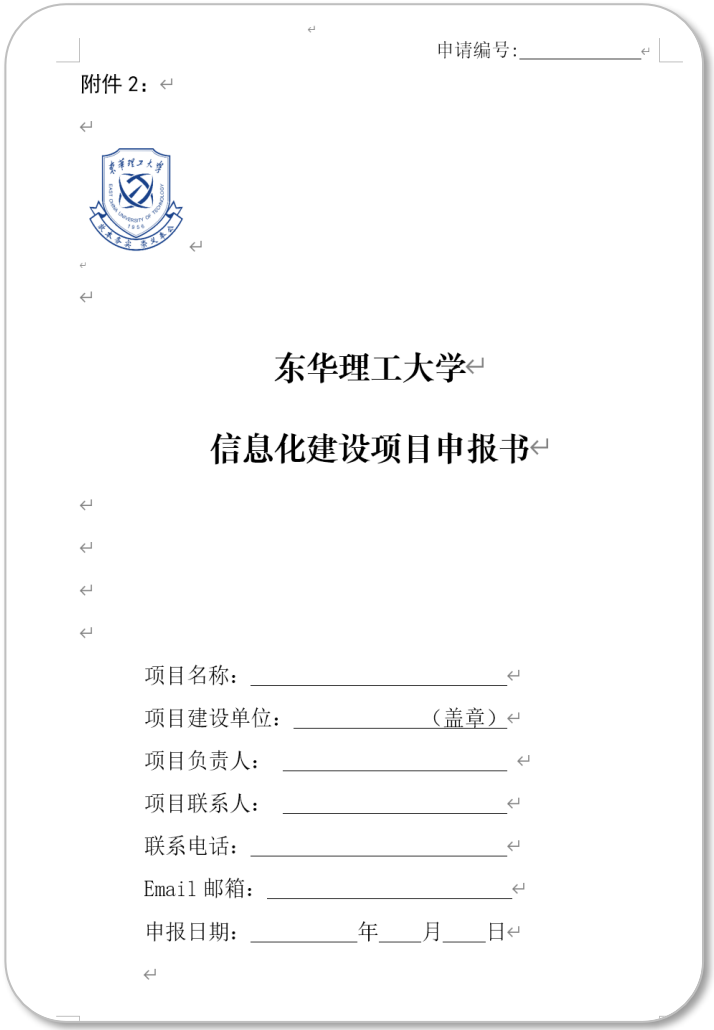
实施范围：校园网整体安全

/04 东华理工实践应用与探索

网络安全与信息化建设“三同步”







申请编号:_____

附件 2：

东华理工大学

信息化建设项目申报书

项目名称：_____

项目建设单位：_____（盖章）

项目负责人：_____

项目联系人：_____

联系电话：_____

Email 邮箱：_____

申报日期：_____年____月____日

构建可视化、可联动的网络安全态势感知平台

全网安全态势可视

资产脆弱性态势可视

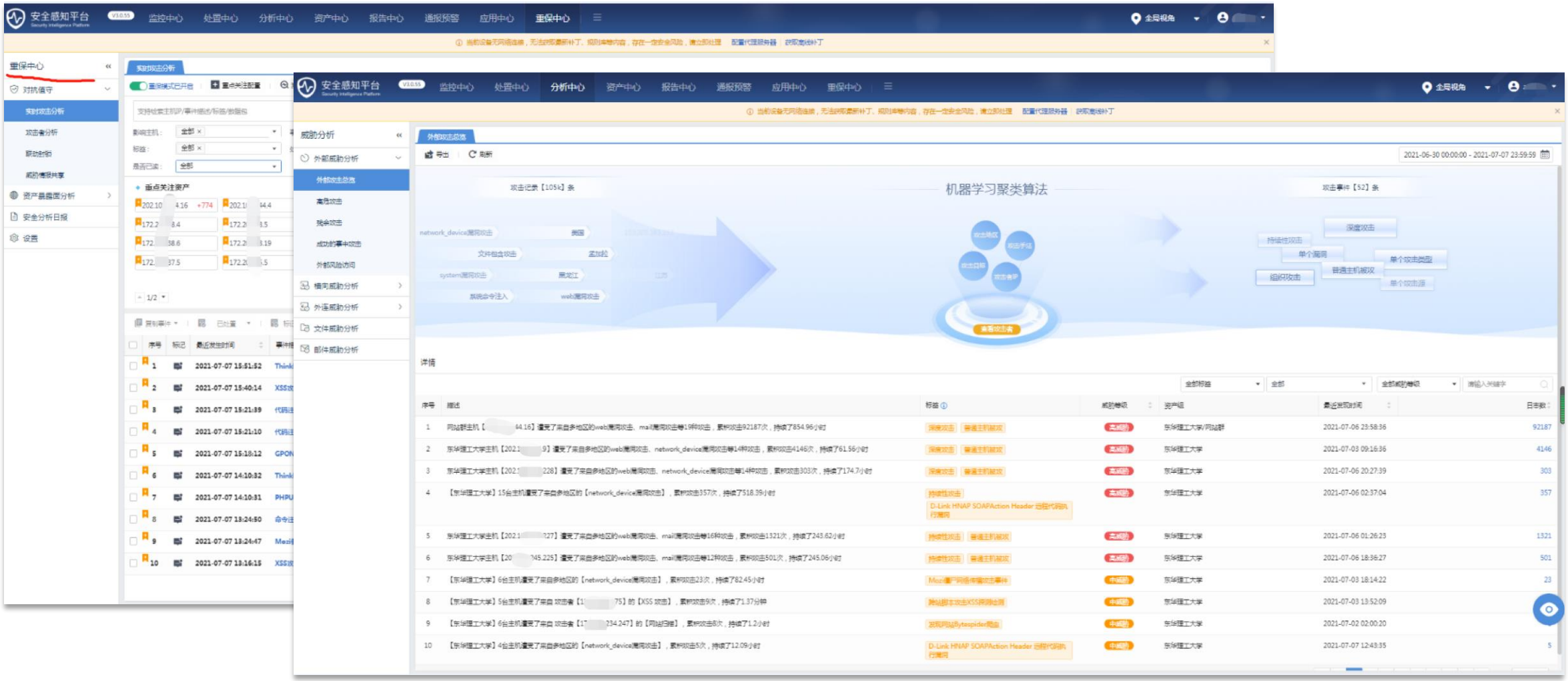
网络攻击态势可视

横向威胁态势可视

安全事件态势可视

分支安全态势可视

提升重保时期发现、控制、管理、追溯攻击行为的能力



组织开展师生网络安全宣传教育与意识技能培训

2020年全校网络与信息安全员集中培训

2020年信息工程学院、软件学院教师网络安全技能培训

2019年江西省第六届“国家网络安全宣传周”校园日活动

2019年江西省第六届“国家网络安全宣传周”校园日活动

举办高校网络安全技能竞赛，发掘培养网络安全人才

2018年第1届江西省高校网络安全技能大赛

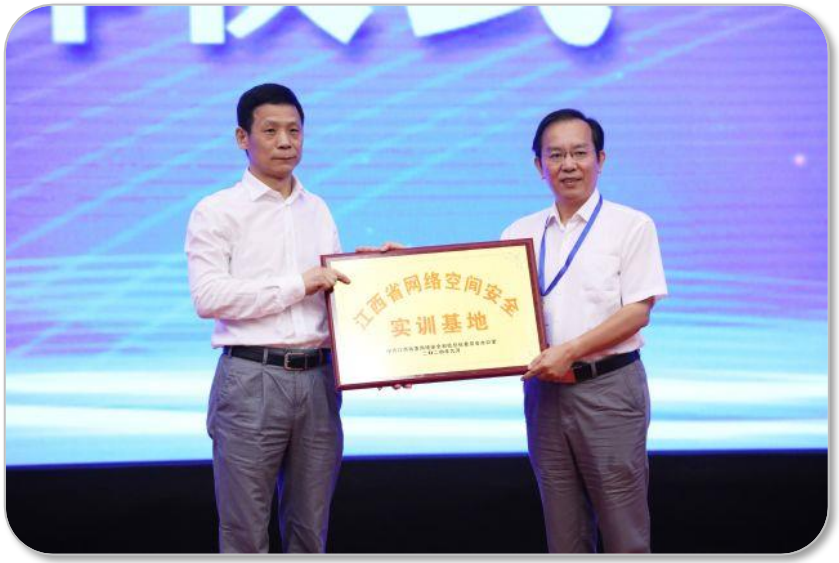
2019第2届江西省高校网络安全技能大赛

2020年第3届江西省高校网络安全技能大赛

2020年第3届江西省高校网络安全技能大赛

创新网络安全人才培养模式，助力网络强国战略

网络与信息中心、信息工程学院联合成立网络空间安全学院，成立江西省首家网络空间安全实训基地，与深信服公司签署《网络空间安全人才联合培养战略协议》，打造“政产学研用”五位一体教育平台



省委网信办主任为学校颁发江西省首家“网络空间安全实训基地”牌匾

与深信服科技公司共建网络空间安全专业，探索校企合作新模式

网络空间安全人才培养创新实验室

THANKS

东华理工大学

欢迎交流、敬请指正