网络安全宣传与培训

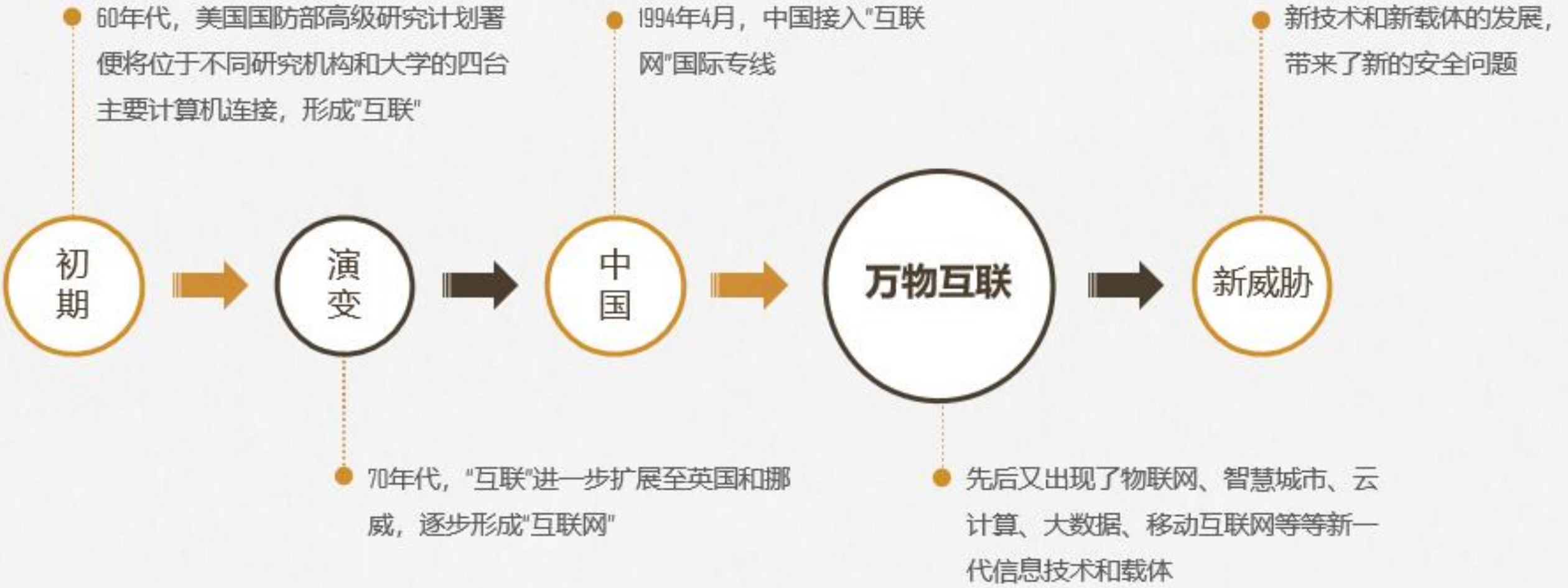
2021年5月26日

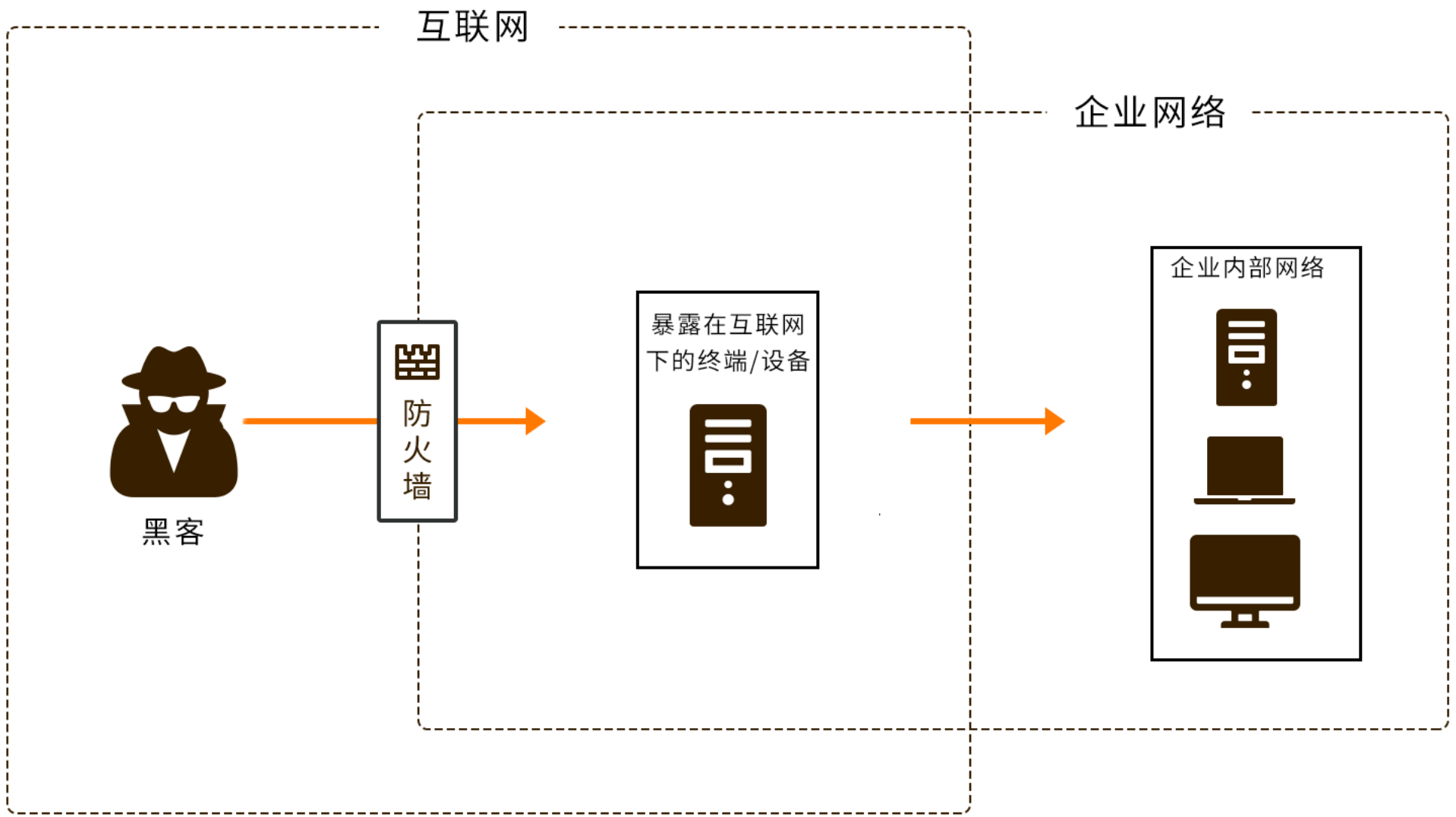
目录

背景介绍

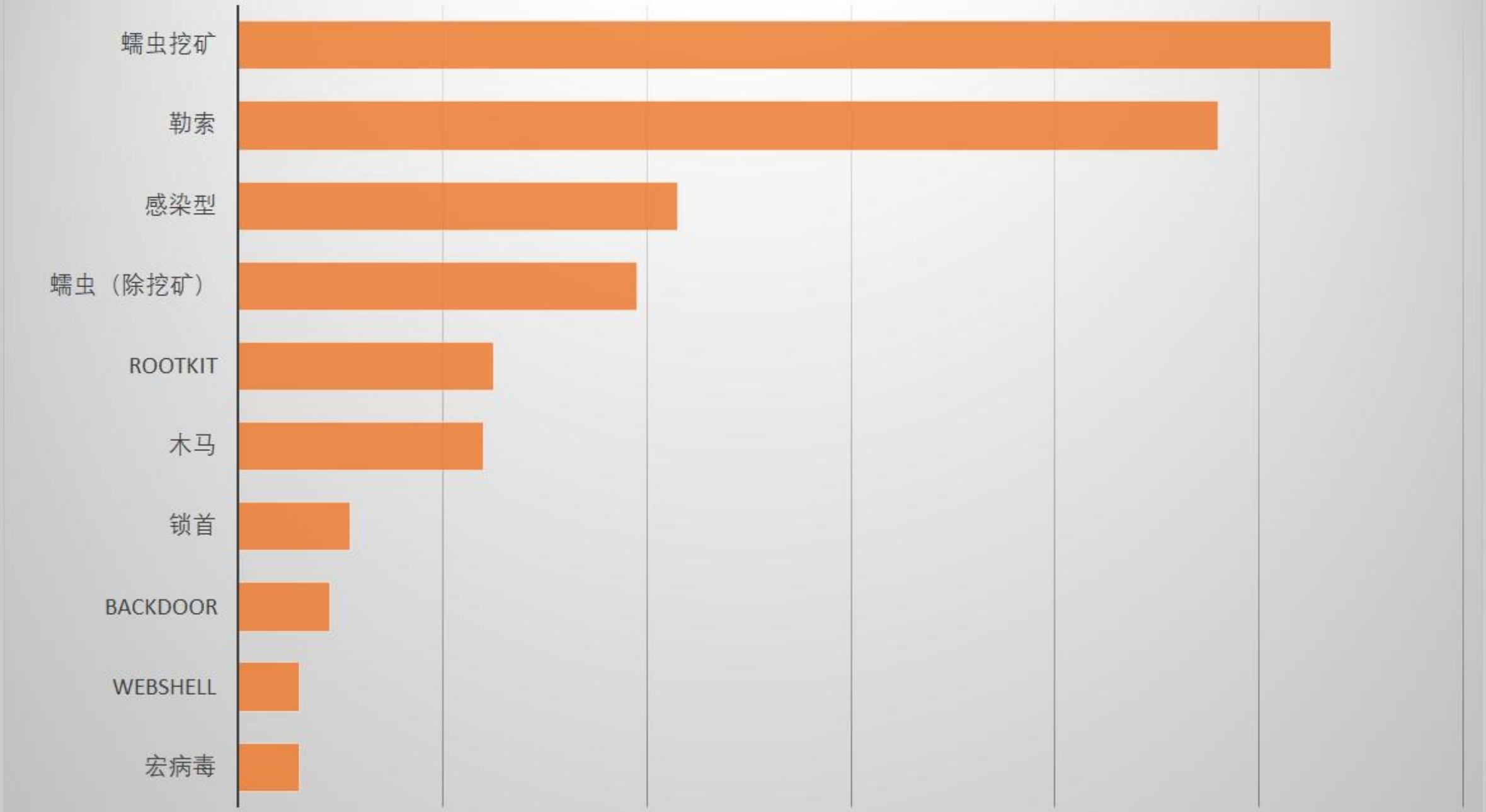
- “十四五”是我国数字化转型的关键阶段，据统计，在十四五规划纲要中“网络安全”一词文中出现了14次，网络安全已成为国家、社会发展面临的重要议题。

- 网络安全不仅关乎国家安全、社会安全、城市安全、基础设施安全，也和社会每个人的生活密切相关。


60年代，美国国防部高级研究计划署便将位于不同研究机构和大学的四台主要计算机连接，形成"互联"
初期
演变
70年代，"互联"进一步扩展至英国和挪威，逐步形成"互联网"
1994年4月，中国接入"互联网"国际专线
中国
万物互联
先后又出现了物联网、智慧城市、云计算、大数据、移动互联网等等新一代信息技术和载体
新技术和新载体的发展，带来了新的安全问题
新威胁


互联网
企业网络
企业内部网络
暴露在互联网下的终端/设备
防火墙
黑客

2020年企业终端主要安全问题



国家网络安全“四个坚持” 的科学内涵与重大意义

要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。

要坚持促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用。

要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。

要坚持安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感。

国家网络安全“四个坚持”

习近平总书记关于国家网络安全的重要指示，充分体现了对网络空间发展规律和形势的深刻把握，体现了以人民为中心的发展思想，以宽阔的战略视野、深邃的历史洞察、深刻的辩证思维，深刻分析了网络空间发展的新形势、新特点、新任务，释放出网络安全为人民、网络安全靠人民的强烈信号，为新形势下做好网络安全工作指明了方向、提供了根本遵循，具有重要的指导意义。

国家网络安全宣传周

网信工作，习近平这样说

党的十八大以来，习近平总书记对网信工作发表了系列重要讲话，提出一系列新理念、新思想、新战略，系统阐述事关网信发展的重大理论和实践问题。

国家网络安全宣传周

一、没有网络安全就没有国家安全

在信息时代，网络安全对国家安全牵一发而动全身，同许多其他方面的安全都有着密切关系。

——2016年4月19日，在网络安全和信息化工作座谈会上的讲话

没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。

——2014年2月27日，在中央网络安全和信息化领导小组第一次会议上的讲话

维护网络安全不应有双重标准，不能一个国家安全而其他国家不安全，一部分国家安全而另一部分国家不安全，更不能以牺牲别国安全谋求自身所谓绝对安全。

——2015年12月16日，在第二届世界互联网大会开幕式上的讲话

二、网络安全为人民

网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

——2014年2月27日，在中央网络安全和信息化领导小组第一次会议上的讲话

做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。

——2014年2月27日，在中央网络安全和信息化领导小组第一次会议上的讲话

三、网络安全靠人民

网络安全的本质在对抗，对抗的本质在攻防两端能力较量。要落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。

——2016年4月19日，在网络安全和信息化工作座谈会上的讲话

要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。

—— 2018年4月20日至21日，在全国网络安全和信息化工作会议上的讲话

网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

——2016年4月19日，在网络安全和信息化工作座谈会上的讲话

1. 网络安全政策与解读

- 《中华人民共和国网络安全法》（中华人民共和国主席令（第五十三号））
- 教育部关于印发《教育信息化2.0行动计划》的通知（教技〔2018〕6号）
- 关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）
- 关于印发《华东师范大学网络安全事件应急预案（2021年修订）》的通知（华师网信〔2021〕2号）
- 华东师范大学网络安全“十四五”规划
- 华东师范大学网络安全发展计划（2021-2023年）

中华人民共和国网络安全法

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）

目　录

中华人民共和国网络安全法_中国人大网 (npc.gov.cn)

信息名称： 教育部关于印发《教育信息化2.0行动计划》的通知

信息索引： 360A16-09-2018-0011-1 **生成日期：** 2018-04-18 **发文机构：** 中华人民共和国教育部

发文字号： 教技〔2018〕6号 **信息类别：** 教育信息化

内容概述： 教育部印发《教育信息化2.0行动计划》。

教育部关于印发《教育信息化2.0行动计划》的通知

教技〔2018〕6号

各省、自治区、直辖市教育厅（教委），各计划单列市教育局，新疆生产建设兵团教育局，部属各高等学校：

为深入贯彻落实党的十九大精神，办好网络教育，积极推进“互联网+教育”发展，加快教育现代化和教育强国建设，我部研究制定了《教育信息化2.0行动计划》，现印发给你们，请结合本地、本单位工作实际，认真贯彻执行。

教育部

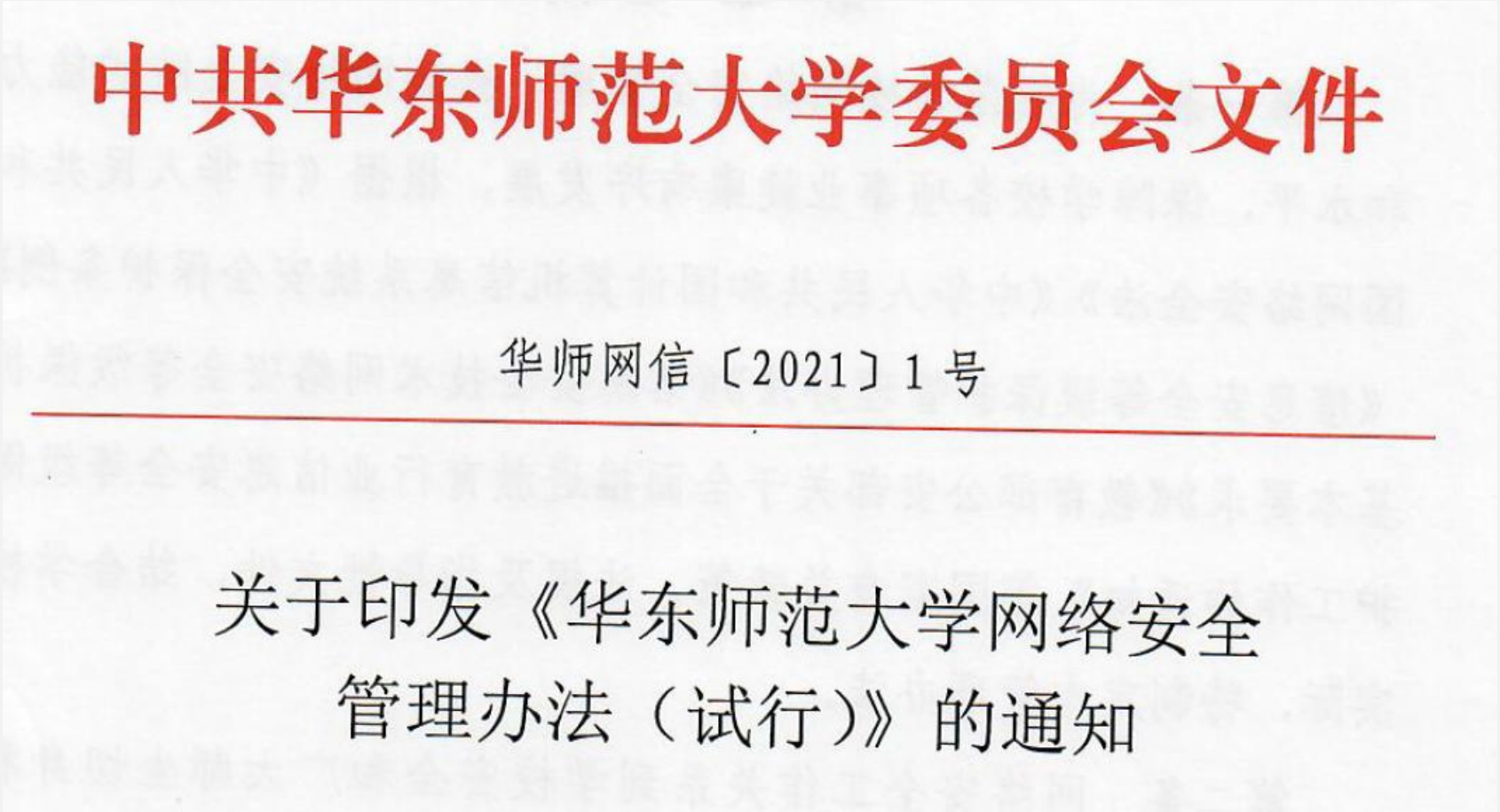
2018年4月13日

三通两平台

- 2012年9月5日刘延东副总理（时任国务委员），在全国教育信息化工作电视电话会议上提出：“十二五”期间，要以建设好“三通两平台”为抓手，也就是“宽带网络校校通、优质资源班班通、网络学习空间人人通”，建设教育资源公共服务平台和教育管理公共服务平台。

- 教育信息化是衡量一个国家和地区教育发展水平的重要标志，实现教育现代化、创新教学模式、提高教育质量，迫切需要大力推进教育信息化。当前和今后一个时期，要大力推进“三通两平台”建设。力争实现四个新突破，即教育信息化基础设施建设新突破、优质数字教育资源共建共享新突破、信息技术与教育教学深度融合新突破、教育信息化科学发展机制的新突破。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）



中共华东师范大学委员会文件

华师网信〔2021〕1号

关于印发《华东师范大学网络安全管理办法（试行）》的通知

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

第一条　为规范学校网络安全管理，提高网络安全防护能力和水平，保障学校各项事业健康有序发展，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《信息安全等级保护管理办法》《信息安全技术网络安全等级保护基本要求》《教育部公安部关于全面推进教育行业信息安全等级保护工作的通知》等国家有关政策、法规及指导性文件，结合学校实际，特制定本管理办法。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

第二条 网络安全工作关系到学校安全和广大师生切身利益，关系到学校教学、科研和管理各项工作的稳定运行，在学校统筹安全与发展工作中具有重要地位。应加强党对学校网络安全工作的领导，发挥党委的政治核心作用，严格落实主体责任，努力形成党委统一领导、党政齐抓共管、有关部门各负其责的网络安全工作格局。

第三条 校内各级党组织要强化政治责任，建立“主要负责人负总责，直接负责人牵头抓”的网络安全领导责任制。按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”和“属地管理，逐级负责”的原则，学校党委负责指导和监管全校网络安全工作，各相关机构、各部处在职能范围内负责网络安全监督管理工作，各二级单位党组织对本单位网络安全工作负主体责任，落实网络安全各项任务。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

第七条　二级单位党组织主要承担以下网络安全职责：

（一）及时传达和认真贯彻学校网络安全工作的决策部署和工作要求，贯彻落实网络安全法律法规和政策文件。

（二）统筹本单位的网络安全建设和管理工作。建立健全网络安全责任制和相关制度规范，落实网络安全管理和防护措施，并将网络安全责任要求落实到本单位各内设机构。

（三）将网络安全工作纳入领导班子重要议事日程，建立健全二级单位党组织领导下的网络安全决策机制，落实相关人力、财力、物力的支持和保障，制定网络安全工作规划，确保网络安全各项任务落实到位。

（四）落实网络安全工作队伍。明确由本单位党组织主要负责人担任网络安全第一责任人，由主管网络安全的领导班子成员担任网络安全直接责任人，由具体分管网络安全的工作人员担任网络安全联络员，各类信息系统（网站）和新媒体账号等由在职教职员工担任管理员，重要系统、平台的管理员应建立工作补位机制，确保相关人员具备第一时间应急响应能力。

（五）落实网络安全清查工作。及时向网信办报送本单位网络安全工作队伍通讯录，向信息办报送信息资产清单，向党委宣传部报备本单位新媒体公众账号清单。

（六）落实网络安全等级保护制度。依法完成所属信息资产的网络安全等级保护定级备案、等级测评、安全建设等工作。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

（七）开展网络安全自查工作。定期组织针对本单位信息系统的安全巡查，对负有主体责任的网络发布内容进行适时跟踪和把关，建立网络安全工作台账。

（八）做好网络安全应急响应工作。配合学校开展本单位网络安全保护和重大事件处理工作，制定网络安全应急预案并定期组织应急演练，发生重大网络安全事件，网络安全负责人应一线指挥，第一时间报告学校信息办、网信办及相关职能部处，并第一时间做好应对处置。

（九）及时汇总并向网信办报告网络安全重大事项。

第三章　网络及信息系统安全

第八条　校园网及相关基础设施由学校统一规划、建设、管理，并提供统一网络出口。校内各单位及个人不得擅自建设、更改、损毁、挪用校园网设施，不得私接外网出口，不得私自提供给校外人员使用。

第十二条　校园网 IP 地址或域名未经许可不得对外提供互联网服务。若需要 IP 地址或域名对外开放服务，应经信息办、网信办审批后方可开放，建设单位承担全部网络安全责任。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

第十四条 各单位负责本单位安装使用的网络打印机、电子显示屏等物联终端及其控制系统的安全防护，应掌握使用情况、落实防范措施、加强安全监管、确保运行安全。

第十五条 终端计算机使用人应做好终端计算机的安全防范，终端计算机上安装、运行的软件须为正版软件，使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第十六条 各单位和教职工、学生使用学校电子邮箱应遵守学校电子邮箱管理等相关规章制度，并对使用其电子邮箱账号开展的所有活动负责，禁止使用电子邮箱传播恶意程序和不良信息，禁止使用电子邮箱存储、处理、传输涉密信息和工作敏感信息。为确保邮箱安全，学校将定期冻结或收回长时间未使用的邮箱。

第十七条 学校信息系统必须符合国家、地方和学校等各级单位有关网络安全的法律法规和制度要求。对于不符合网络安全要求的信息系统必须先进行整改，整改完成后方可提供服务。

第十八条 未经信息办、网信办审批备案的信息系统不属于学校信息资产，不得使用学校相关信息化资源，不得使用校名、校徽等学校标识，一切网络安全责任由系统建设、使用单位或个人承担。

第十九条 IP 地址或域名需对外开放的应用服务，应按照国家法律法规要求开展相应网络安全等级保护（以下简称安全等保）工作。信息办负责校内信息系统安全等保工作的组织协调，各单位负责本单位主管信息系统安全等保工作的具体落实。

第二十一条 各单位应强化供应链安全管理，采用安全规范、质量和售后服务优良的软硬件产品并选择服务优质、资质和信誉良好的服务厂商承建信息系统建设项目，优先选用具有自主核心技术以及安全性达到要求的国产化产品。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

第二十二条 各单位应加强信息技术外包服务的安全管理，对外包服务全流程实行严格监督和管理，确保外包服务的连续性和安全性。

第二十三条 各单位应加强信息资产管理，规范信息资产的新增购置、日常运维和更新替代，形成信息资产清单，有效保障信息资产安全。

第二十四条 新建信息系统项目立项时应将安全运维与安全等保测评费用纳入预算。新建信息系统项目中的人员、经费、采购、合同、建设、验收、运维等各环节中都需包含网络安全相关说明。

第二十五条 新建信息系统项目验收前必须通过必要的安全检测，未通过检测不得验收。新建信息系统如需面向互联网开放，必须通过安全等保测评。

第二十六条 各单位应加强源代码安全管理，在信息系统上线运行前或者发生重大变化时须进行系统源代码安全审查。

第二十八条 各单位门户网站及其它各类文章发布类信息系统，应统一基于学校网站群平台进行建设。信息办负责网站群平台的建设、管理和运维，提供建站技术支持，各单位负责网站的规范运行和内容安全。

第二十九条 原则上各单位不得再建设使用校外 IP 地址或校外域名提供学校相关服务的系统。对于现使用校外 IP 地址或校外域名提供学校相关服务的系统须每年进行审查，如有不符合网络安全规定者限期迁至校内或关停。相关责任单位应落实安全等保要求，或将系统迁移纳入学校统一管理。

关于印发《华东师范大学网络安全管理办法（试行）》的通知（华师网信〔2021〕1号）

第三十一条 各单位应加强信息系统的数据安全，对重要数据做好定期完整备份和实时增量备份，确保重要数据资源不被破坏、篡改和泄露。涉及学校基础数据、教职工和学生个人信息或敏感信息的信息系统，不得部署在校外。未经批准，严禁使用境外数据中心存储数据。

第三十二条 各单位应按照国家有关法律法规的规定严格保护学校师生个人信息，不得违规采集、存储、使用和处理校内各类个人信息。

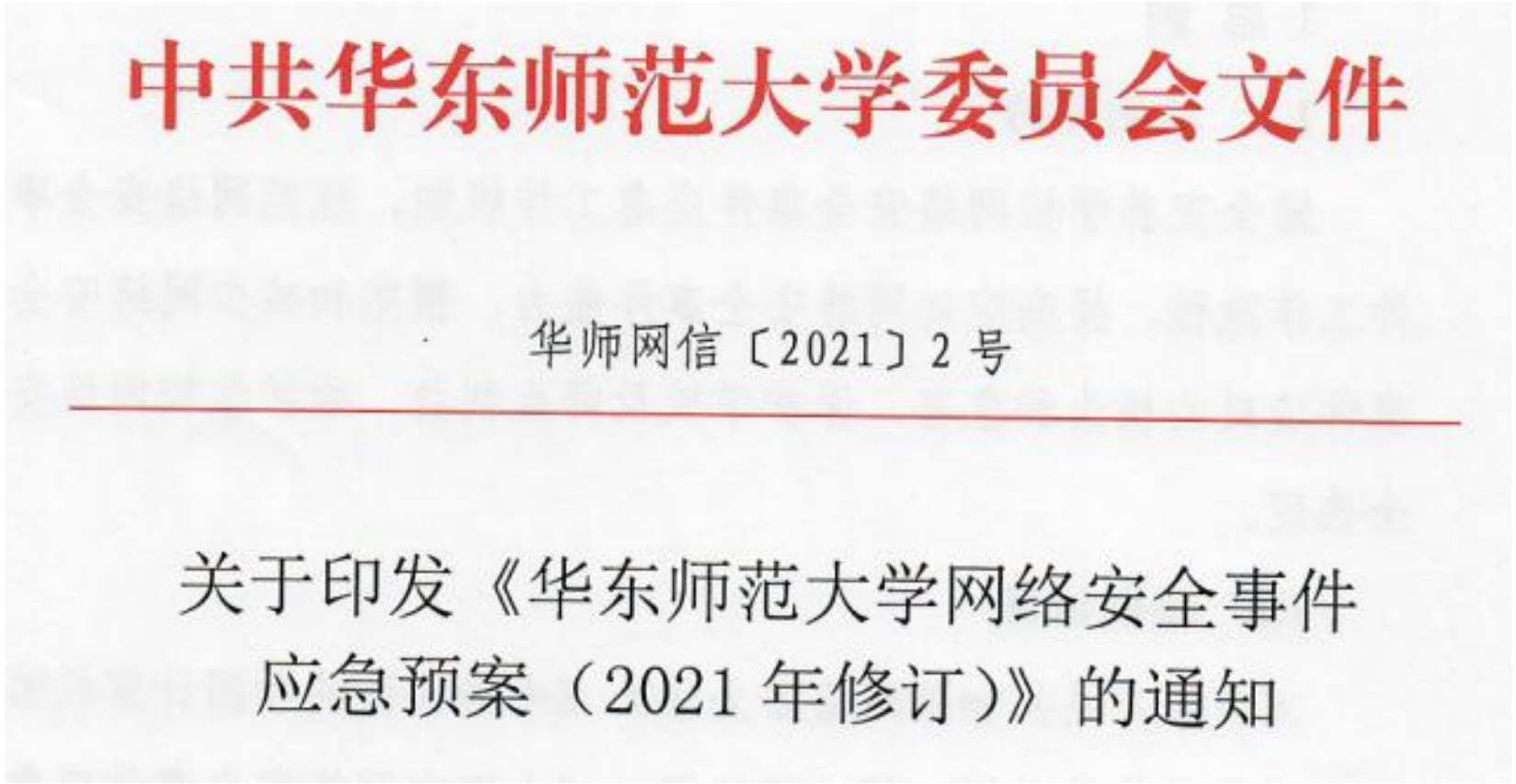
第三十三条 各类信息系统使用者应加强账户安全管理，杜绝使用弱密码、默认密码和通用密码。关键岗位的信息系统使用和管理人员应签订网络安全保密协议。离岗、离职人员的访问权限应及时予以终止。

第四十一条 各单位每年需安排每位在职人员完成不少于 4 个学时有关网络安全的学习与培训任务，并纳入教职工政治理论学习统筹管理。其中，集中学习、研讨 1 学时，自主学习 3 学时及以上。

第四十二条 各单位组织的网络安全学习与培训可采取线下和线上等多种形式：既可组织线下的网络安全法规的学习，进行网络安全知识和技术的培训；也可依托网络资源组织线上学习，听取专题报告、开展线上专题研讨等。

第四十三条 各单位需指定专人对学习和培训进行通知和管理，并负责记录本单位的学习和培训情况台账。

关于印发《华东师范大学网络安全事件应急预案（2021年修订）》的通知（华师网信〔2021〕2号）



中共华东师范大学委员会文件

华师网信〔2021〕2号

关于印发《华东师范大学网络安全事件应急预案（2021年修订）》的通知

关于印发《华东师范大学网络安全事件应急预案（2021年修订）》的通知（华师网信〔2021〕2号）

网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

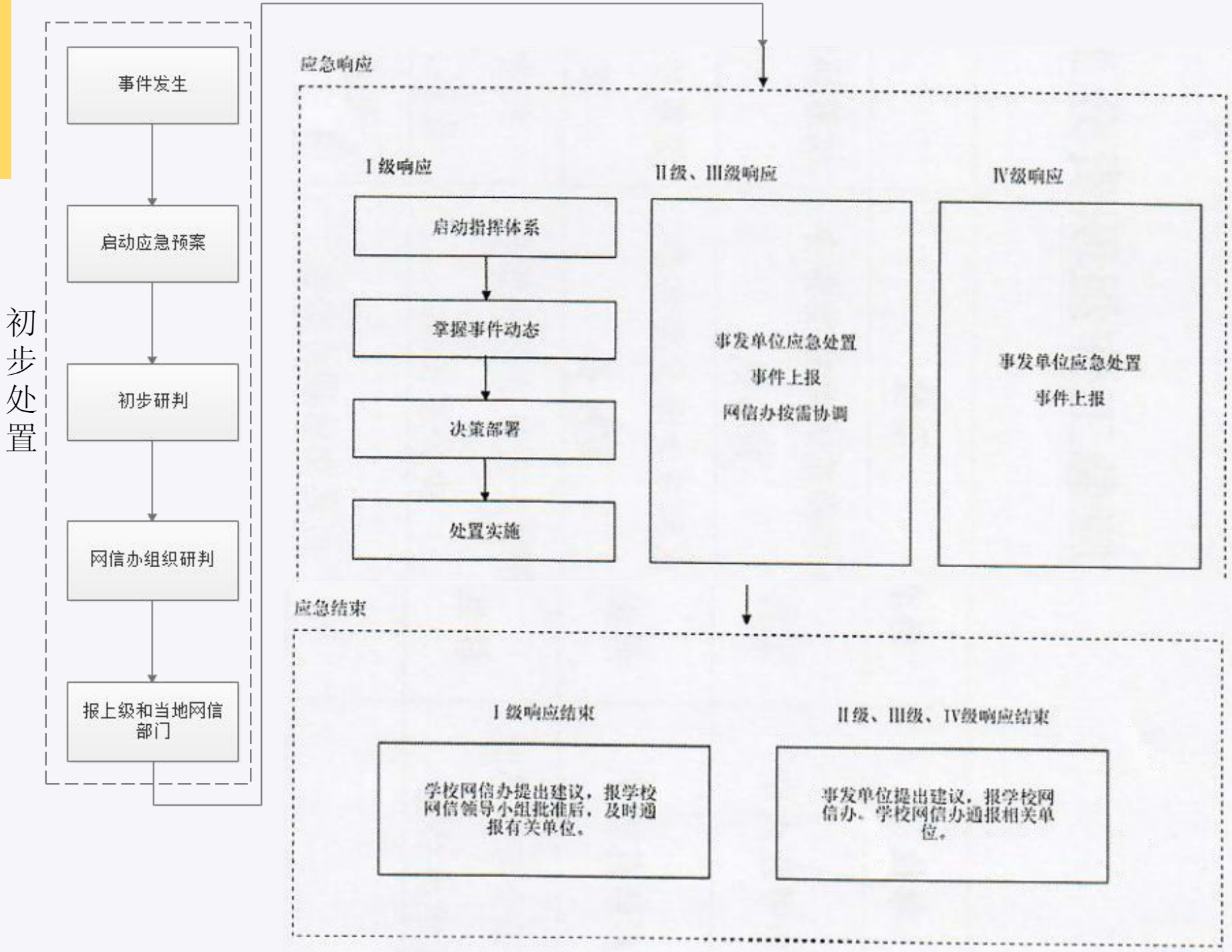
（4）信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

应急处置工作流程


初步处置
事件发生
启动应急预案
初步研判
网信办组织研判
报上级和当地网信部门
应急响应
Ⅰ级响应
启动指挥体系
掌握事件动态
决策部署
处置实施
Ⅱ级、Ⅲ级响应
事发单位应急处置
事件上报
网信办按需协调
Ⅳ级响应
事发单位应急处置
事件上报
应急结束
Ⅰ级响应结束
学校网信办提出建议，报学校网信领导小组批准后，及时通报有关单位。
Ⅱ级、Ⅲ级、Ⅳ级响应结束
事发单位提出建议，报学校网信办。学校网信办通报相关单位。

网络安全微课展播

- https://www.gjwlaqxcz.cn/weike

冒充公检法诈骗

作者：尔玉 喵喵反诈骗小分队

坑人的包过考题

作者：蛋蛋 喵喵反诈骗小分队

新型套路贷

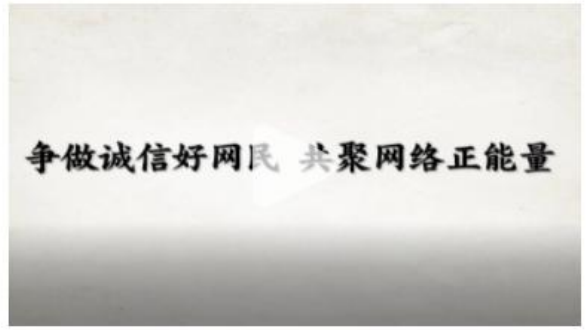
作者：贝儿 喵喵反诈骗小分队

键盘篇

作者：蒋亚清

网聚“郑”能力 守护“她”安全宣传片

作者：郑州市妇女联合会



好网民

作者：崔怀阳

安全小课堂 & 安全微视频

网络安全宣传 (xuexi.cn)

数字经济时代

数字技术助推网络安全 (xuexi.cn)

网络安全软件的一般功能

终端登录防护

身份校验 拦截

灵活的网络管理

IP协议控制 黑名单

漏洞攻击防护技术

“虚拟补丁”“热补丁”

全面的系统加固

文件防护 注册表防护 敏感动作防护

恶意代码检测处置

检测发现 拦截处置

资产登记与管理

统一管控 安全审计

数据备份

- 为确保数据安全，请定期备份数据!
- 方法:
  - 复制到移动硬盘（机械硬盘、刻录光盘、网络硬盘等）
  - 数据压缩（zip、rar、专用格式等）
- 推荐软件:
  - Fastcopy、360压缩、7-zip等
- 请勿购买和使用劣质存储介质：推广赠送的U盘、淘宝二手硬盘、部分厂商的入门级固态硬盘等。

相对可靠的硬盘品牌

- U盘、存储卡：Sandisk、雷克沙、三星、东芝、爱国者、朗科
- 机械硬盘：西部数据（WD）、希捷（Seagate）
- 固态硬盘：镁光（Crucial）、三星、东芝、西部数据、Sandisk、致钛（自研优秀国产品牌）、浦科特、威刚（ADATA）

- 同时尽量避免入门级产品

数据恢复

- 为避免数据恢复，请定期备份数据！如果需恢复数据，请立刻对相关存储介质安全断电！
- 数据恢复并非100%成功，甚至只有30%左右的有效数据可恢复。
- 数据恢复是专业工作，包括存储卡恢复（TF、SD等）、硬盘恢复（机械硬盘、固态硬盘等），请到正规具有资质的公司恢复，并注意数据保密（合同约定）。

- 数据恢复相对昂贵，个人平均花费500~10000RMB，费用能购买若干数量的优质硬盘。

数据恢复

- 故障类型一般分为逻辑故障和硬件故障。
  - 逻辑故障：删除、格式化、分区丢失、文件打开乱码等等，同样是删除，普通的office文件，价格较低。要是数据库文件等特殊结构的文件，价格就不只这些了，文件结构不一样，存储原理不同，难度不同。
  - 硬件故障：如摔、磕碰、断电、USB口供电电压不稳等导致硬盘出现坏道、存储颗粒损坏导致无法读取数据，还有固件丢失、BUG等问题。

交流讨论

感谢聆听