制定自主网络安全体系框架的国家标准迫在眉睫

奇安信集团董事长 齐向东

目录

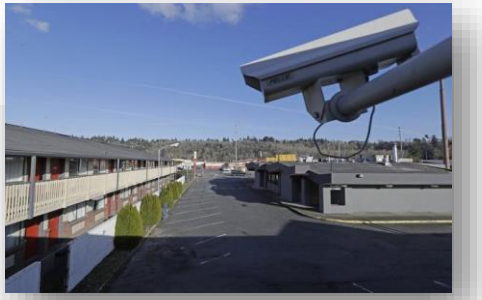
挑战一：供应链暗雷重重

软件测试工具被植入恶意代码，影响全球2.9万名客户

- 2021年4月，软件单元测试覆盖度统计工具codecov遭到攻击，统计脚本程序被植入恶意代码，用于窃取软件的密钥、密码等凭证，已经导致数百个客户的网络被访问。该工具覆盖的客户规模高达2.9万，包括谷歌、IBM、宝洁等多家知名企业。

供应商被黑，特斯拉及15万监控摄像头数据遭泄露

- 2021年3月，黑客组织攻陷了特斯拉摄像头供应商Verkada，通过“超级管理员”账户获得了访问权限，特斯拉以及美国监狱、警察局、医院和学校等15万个监控摄像数据遭泄露。

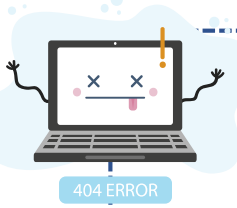


金链熊：美国“史上最严重”供应链攻击，至少有200家重要机构受害

- 2020年12月，奇安信披露了年度最严重的APT事件，全球知名软件厂商“太阳风”(SolarWinds) 遭“金链熊”黑客组织攻击，至少200家重要机构受害。其中，美国受害最严重，美国国土安全部、财政部、核安全管理局等多个重要机构都受到波及。

挑战一：供应链暗雷重重

供应链三大环节存风险，开源软件和源代码暗藏危机



- 供应链可划分为**开发**、**交付**、**使用**三个大环节，**每个环节都可能会引入供应链安全风险**从而遭受攻击，上游环节的安全问题会传递到下游环节并放大。
- 我国企业在开发阶段广泛应用**不安全的开源软件，自主开发的程序天然存在缺陷**，对供应链安全造成巨大威胁。

开发环节（厂商）

- 开源组件漏洞问题比较多，依赖关系复杂
- 程序员编码问题（漏洞/后门）
- 编译环境污染问题

交付环节（代理商、集成商）

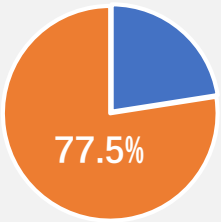
- 下载源可靠性问题
- 代理商交付中间环节引入恶意代码
- 损害软件的完整性

使用环节（用户）

- 软件更新被劫持问题
- 正常软件版本被插入恶意代码

采用开源软件项目
每个项目平均有52.5个漏洞

奇安信**开源卫士**对**2188个软件**开发项目进行了调研，**100%**的项目都用了**开源软件**。其中有**1695个**项目存在开源软件漏洞，占比高达**77.5%**。



平均**每个项目**有**52.5个**开源软件漏洞

自主开发的程序
每1000行代码平均有10.13个缺陷

- 奇安信**代码卫士**对**1838个软件**项目的源代码进行了分析，**代码超3亿行**，发现**330万**个安全缺陷，高危安全缺陷**36万**个。
- 我国**73%的程序员工作年限不到5年**，代码容易出现纰漏，留下漏洞。
- 统计显示，程序员每敲**一千行**原始代码，会出现**10.13个缺陷**，其中有**1.08个高危缺陷**。

挑战二：漏洞不可避免

高通芯片曝出高危漏洞，全球40%的手机受到影响

- **2021年5月**，高通的MSM芯片被曝存在高危安全漏洞（CVE-2020-11292）。报道称，目前高通2G、3G、4G、5G的系列芯片，全部存在此漏洞，攻击者可以利用该漏洞获取用户隐私信息，甚至监听用户通话，将手机变成监控设备。作为向三星、LG、小米等多个手机品牌供货的芯片大厂，高通这个高危漏洞让全球40%的手机用户暴露在了危险之下。

戴尔曝出高危漏洞潜伏12年，数亿台电脑受影响

- **2021年5月**，戴尔披露其上亿台电脑的固件升级驱动中存在一个潜伏了长达12年的高危漏洞，该高危漏洞由访问控制不足引起，极有可能引发信息泄露，或被攻击者利用进行DDoS攻击，对全球数亿台电脑造成严重影响。

VMware漏洞威胁美国国家安全

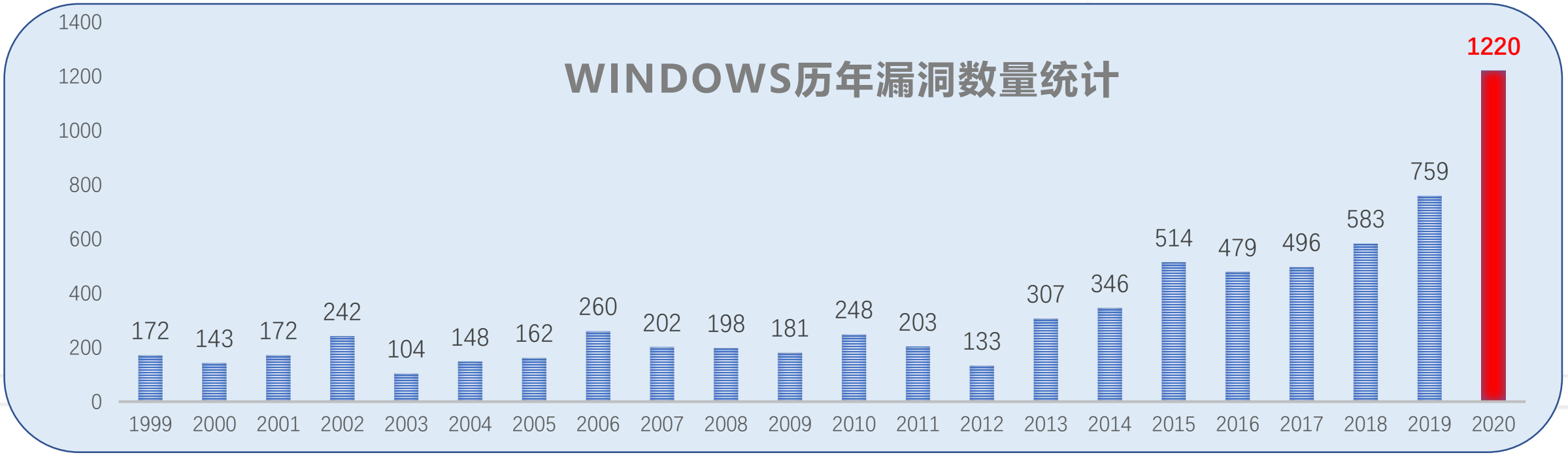
- **2020年12月**，美国国安局发出警告，黑客组织正在利用CVE-2020-4006VMware漏洞进行网络间谍活动。黑客可以利用该漏洞访问被攻击系统，执行自己选择的命令。

利用蓝牙漏洞获取物联网设备权限

- **2020年10月**，蓝牙协议栈BlueZ被曝存在高危漏洞，黑客不需要经过身份认证，就能通过特定输入进行“零点击”攻击，从而获取物联网设备权限。

挑战二：漏洞不可避免

- 1999年-2020年，Windows平台**提交漏洞总计7272个，2020年是1999年的7.1倍。**
- 疫情按下了全球数字化的加速键，也让更多的漏洞暴露出来。统计数据显示，Windows平台提交漏洞数量暴增，**2020年达到了1220个。**



挑战三：勒索攻击泛滥成灾

- 2021年预计**每11秒将发生一次勒索攻击**，全年**超300万次。**——美国安全机构Cybersecurity Ventures
- 2020年，勒索软件的**平均赎金达到31万美元**，是1989年的**1640倍。**——美国安全公司Palo Alto的报告

勒索病毒通过变种，躲避安全软件的封锁

例如，GlobeImposter勒索病毒“十二主神”首次出现于2017年，在近三年演化了多个版本。2020年，该病毒的全新变种出现，锁住目标主机的系统和文件，勒索赎金，同时躲避安全软件的封锁。

苹果代工厂遭勒索
被索要3.25亿赎金

➢ **2021年4月**，黑客通过勒索攻击，**窃取了苹果的设计蓝图**，索要**5000万美元（约3.25亿元）赎金。**

宏碁遭勒索攻击
赎金达全年净利1/4

➢ **2021年3月**，宏碁电脑被REvil勒索软件攻击，**被索要5000万美元（约3.25亿）赎金**，是宏碁**全年净利的1/4。**

起亚遭勒索攻击
赎金高达2亿元

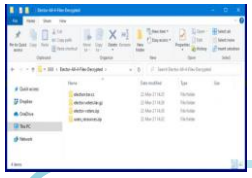
➢ **2021年2月**，起亚汽车遭勒索，黑客要求支付**1.35亿赎金**，若**当天不支付**，将**追加至2亿元。**

挑战四：数据泄露风险暴增

- 2020年全球公开报告了**3932起**数据泄露事件，**370亿条**数据遭到泄露（美国安全服务商Risk Based Security）
- 2020年全球数据产生量预计达**470亿TB**，2035年总数据量将超过**2万亿TB**（中国信通院2020年大数据白皮书）

上亿用户支付数据泄露严重威胁人们财产安全

➢ **2021年4月**，印度国内最大的数字支付运营商之一MobiKwik被曝遭遇黑客攻击，泄露了约1亿用户的个人信息，包括电话号码、邮箱、签名、交易日志、部分付款卡号、密码哈希以及个人身份证明文件。



以色列遭遇最严重数据泄露650余万选民信息全部曝光

➢ **2021年2月**，以色列遭遇有史以来最严重的数据泄露事件，650余万选民的信息遭到泄露，包括全名、电话、住址、性别、政治倾向等详细个人资料。如果这些数据被用于精准推送，将可能改变以色列政治格局。

安全运营缺失，泰国运营商数据持续泄露三周，总量达83亿

➢ **2020年5月**，由于缺乏安全运营，泰国最大移动运营商发生了长达三星期的数据泄漏事件。安全人员未及时发现被泄露的数据库，导致数据每天以几亿条的速度泄露，最终数据泄露总量达到了83亿条。

挑战五：“内鬼”防不胜防

超过85%的网络安全威胁来自于内部

- FBI和CSI等机构联合做的一项安全调查报告显示，超过85%的网络安全威胁来自于内部，危害程度远远超过黑客攻击和病毒造成的损失。

运营商内鬼倒卖微信号250万
非法获利8700万元

- **2021年4月**，央视报道称某犯罪团伙盗用客户信息倒卖。该团伙成员有9人，其中5人是某通讯运营商公司内部员工。自2020年10月至2021年1月，该团伙盗用公民信息，倒卖微信号250万个，非法获利8700万元。

香港电信公司技术员
非法泄露20余名警员信息

- **2020年10月，**香港一名电信公司技术员涉嫌利用工作之便，非法获取超过20名警务人员及警员家属信息，之后向Telegram（即时通讯软件）一群组帐户管理人“报料”，并发布一名警察父亲的个人资料。

黑客买通推特员工
劫持美国多名知名人士账户

- **2020年7月，**黑客买通一名推特员工，获得该员工凭证的控制权，劫持了多位知名人士的账户，包括美国现任总统乔·拜登、前总统巴拉克·奥巴马等。这些账户发布了一模一样的推文，声称如果向其比特币账号地址转账，将在30分钟内以双倍数额返还。

实网攻防演习的经验表明没有打不透的“墙”

有组织的网络攻击，一般会**组合利用**多个**薄弱环节**

1、外网非法连接隔离网
（大量业务应用存在于外网，业务数字化转型、新型技术的深入应用，都在模糊边界，冲击隔离网络这种安全措施）

2、利用内鬼突破隔离网
（当应用没有外联口子的时候，通过钓鱼、社工等方式，利用人的行为突破隔离，挑战网络安全）

3、过分依赖物理隔离，内网安全手段缺失
（因对“物理隔离”的绝对信任，内网缺乏控制措施，一旦突破边界就为所欲为）

4、口令策略缺失，造成失陷灾难
（服务器多，设备多，运维压力大，滋生弱口令、口令同置问题，一台失陷、全部失陷）

5、内网域控薄弱，网管权限高（与互联网链接的网络，对安全关注更高，会做较好的区域划分，很多单位的内网仅根据功能分为2-3个区域，且没有访问控制，一旦失陷影响范围更大）

6、内网应用系统脆弱
（相比外网，主观认识更安全，从而忽略应用安全开发、安全评估与安全审计，导致攻击人员进入内网后发现系统更好突破）

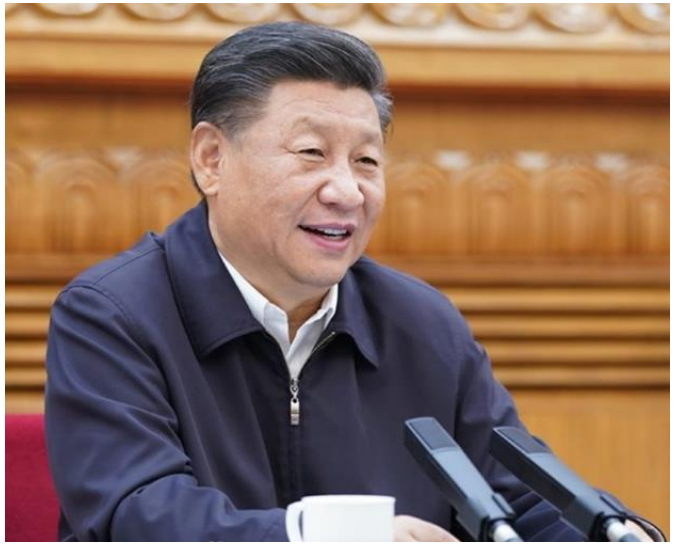
7、供应链中间件存在漏洞
（各类应用用了大量中间件，并采购的大量第三方系统，疏于升级管控，存在漏洞）

8、源代码泄露检测难、打击大
（如果攻击人员在开发商、测试环境中找到内网业务系统的源代码，可以找到业务逻辑漏洞(0day)，会对业务造成致命打击，且不可检测）

9、物联网设备、哑终端设备扩大攻击面
（摄像头等物联网设备，被专项攻击的可能性大，黑客通过外部哑终端接口接入也可能造成接入风险（如与酒店对接的这类系统）

10、内网态势感知能力弱
（缺乏对内网网络、主机层面的监测能力，谁进来了不知道、是敌是友不知道、干了什么不知道，长期“潜伏”，一旦有事就发作了。）

唯有完整的安全体系才能应对新时代的网络安全挑战



习近平总书记多次就网络安全工作作出重要指示

没有网络安全就没有国家安全。

网络安全和信息化是一体之两翼、驱动之双轮。

网络安全是整体的而不是割裂的，网络安全是动态的而不是静态的，网络安全是开放的而不是封闭的，网络安全是相对的而不是绝对的，网络安全是共同的而不是孤立的。

窟窿是补不完的，建立完整的网络安全体系迫在眉睫！

攻防对抗

内外勾结

0Day漏洞

资产暴增

管理混乱

目录

建设完整的网络安全体系面临的两大挑战

挑战一：有愿望、没思路

- 无法确定安全建设方向
- 安全涉及内容太多，无从下手
- 可选方向过多，不知如何选择
- 多种可能，无法达成内部共识

挑战二：有思路、没方法

- 内部对安全体系落地信心不足
- 缺乏合适的资源配置
- 缺乏落地路径和策略
- 相应机制不了解，推进迟缓

挑战的本质是缺乏自主网络安全体系框架

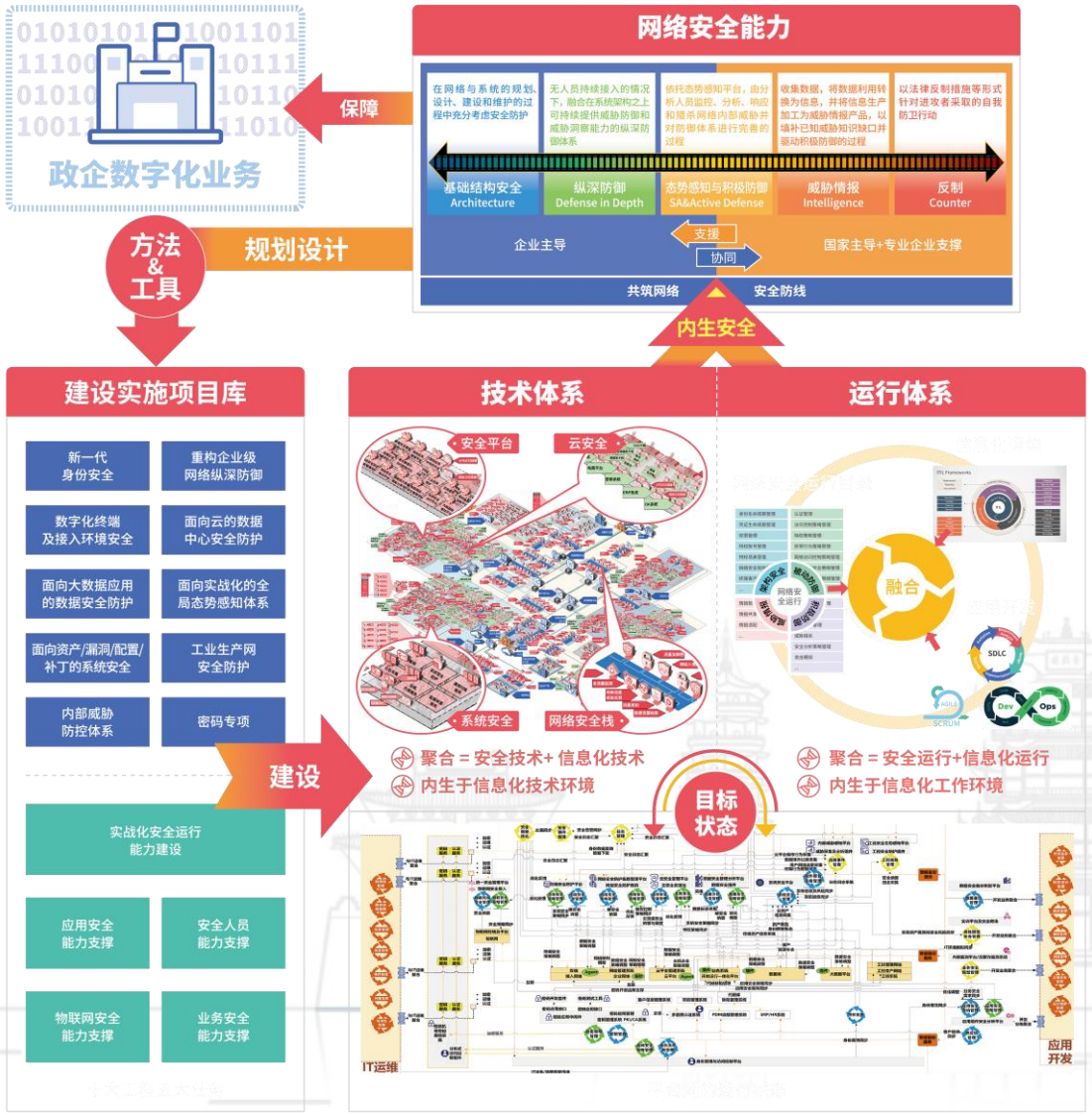
- **网络安全缺乏体系化的根源：**

在理论层面**没有**与企业架构（EA）、运维管理（ITIL）同等层次的、以系统工程思想引导的规划与建设实践，导致网络安全建设以“局部整改”为主，主要是买盒子应对检查。

- **建立网络安全体系的最大缺失：**

没有拉出安全能力体系的全景，**没有**资源保障，**没有**逐步落地的举措。

自主网络安全体系框架给思路、给方法

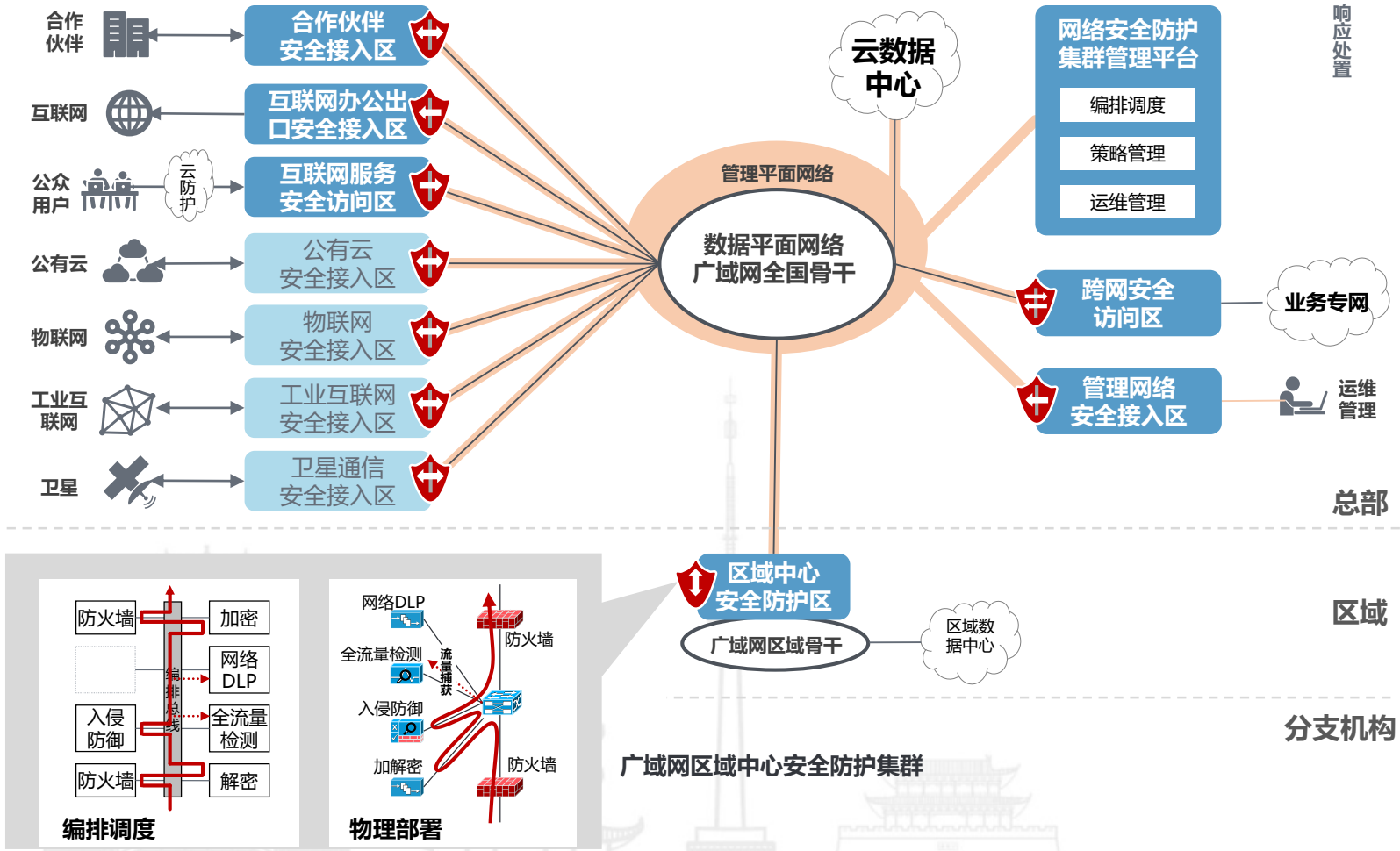


自主网络安全体系框架

- 给思路：以系统工程改变过去局部整改、辅助配套的建设模式，系统化建设完整的网络安全体系。
- 给方法：以具体的工程和任务引导网络安全体系的规划、建设与运营。
- 随着具体工程和任务的落地，政企机构将拥有体系化网络安全能力，从而实现保障数字化业务的目标。

关键一：盘家底

- ✓ **网络基础设施：**
  广域网 局域网 子网 不同域 不同段
- ✓ **云基础设施：**
  私有云 公有云
- ✓ **大数据中心：**
  业务数据中心 灾备数据中心等
- ✓ **应用系统：**
  业务系统 财务系统 ERP等
- ✓ **用户：**
  领导（高密级）员工（普通级）



梳理出总资产数据库：网络拓扑、数据结构、资产类型、资产总量等

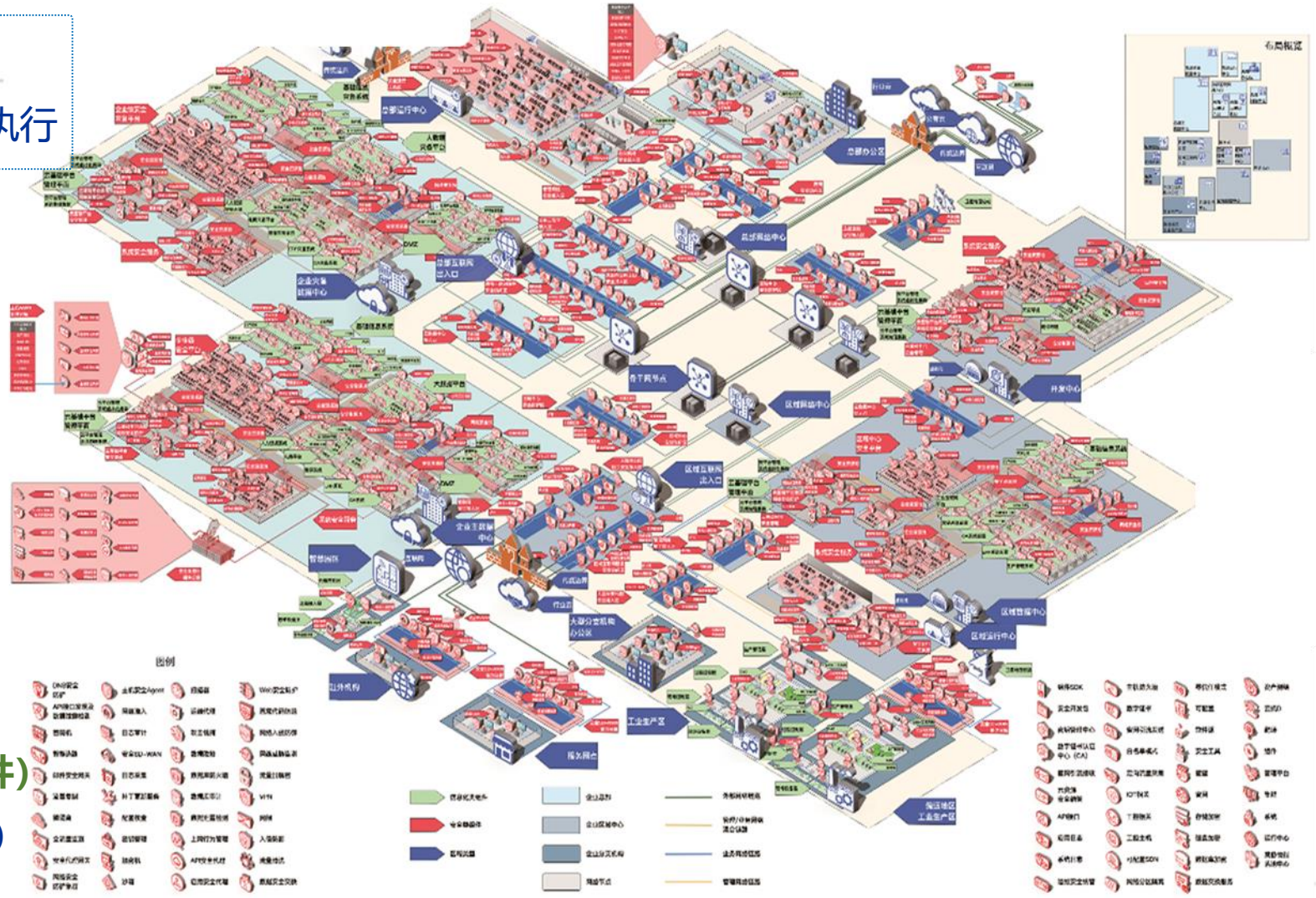
关键二：建系统

- 网络区域众多，产品、接口、标准都不同
- 产品无法协同，数据无法连通，指令无法执行

“安全能力组件化，分别以系统、服务、软硬件资源的形态，科学、有序地部署到信息化环境的不同区域、节点、层级中，确保安全能力可建设、可落地、可调度。”

某“新基建”项目

- 136个信息化子系统（组件）
- 29个业务场景（安全区域）
- 79类安全能力组件

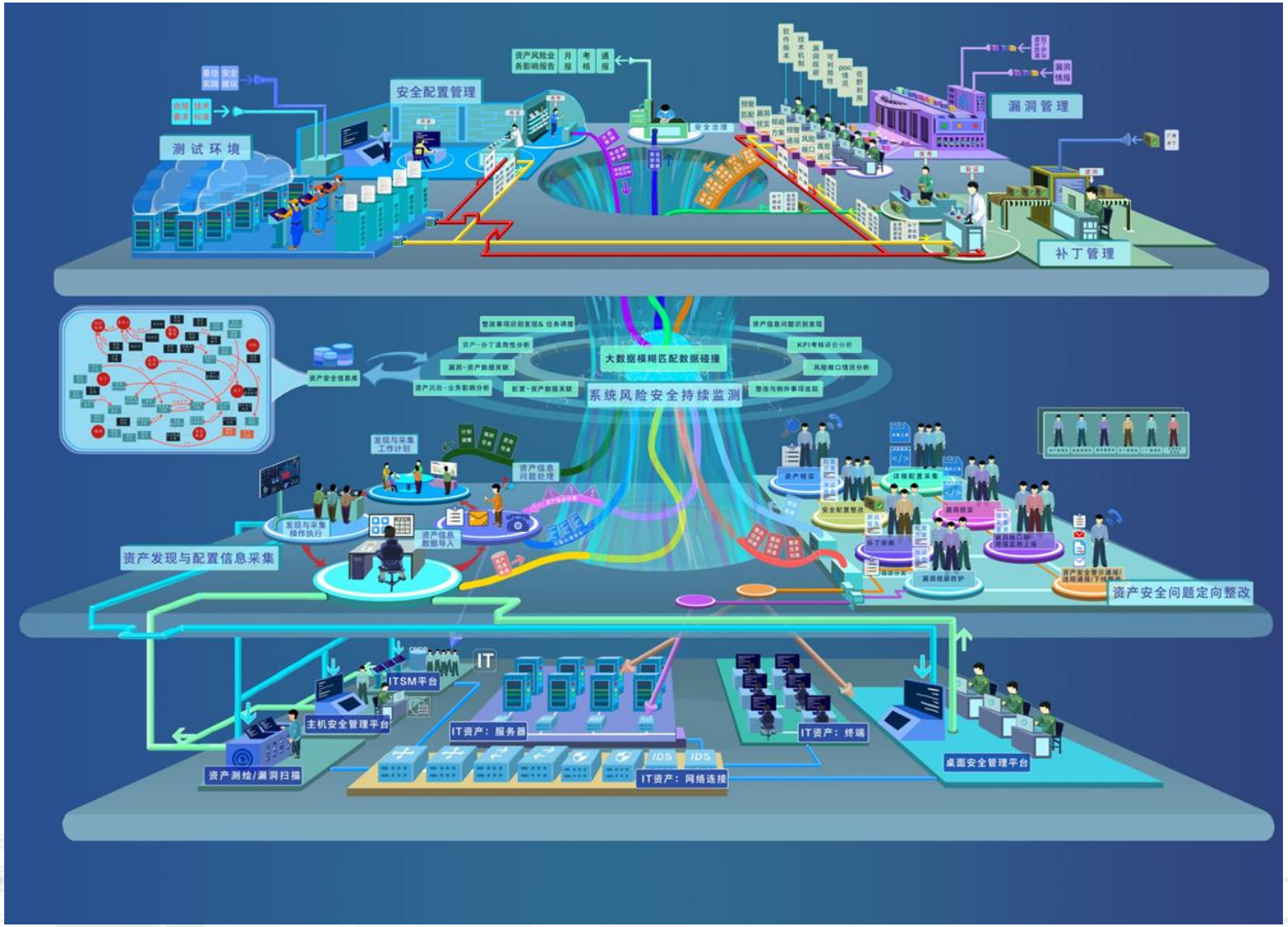


关键三：抓运营

“只有抓安全运营，才能跑得赢漏洞、跑得赢内鬼、跑得赢黑客”

运营的核心是互相连通

- ✓ 常态化的安全工作
- ✓ 事件处置与应急响应
- ✓ 溯源与反制



目录

建议一：制定安全能力建设体系标准

- 确保安全能力完整性：能力组件全面覆盖政企安全机制、技术手段、安全系统、安全管理制度、安全责任等内容，确保所需安全能力完整性。
- 明确IT与安全的融合：将安全能力映射成可执行、可建设的网络安全能力组件。在信息化的所有层面实现安全能力对信息化的覆盖性、融合性。
- 确保安全能力的关联性：各类安全的能力相互协同、互为支撑，形成协同联动、整体防护，避免安全能力之间的割裂导致的碎片化与低效率。

建议二：制定关键技术产品体系标准

- 实现对关键技术和产品的查漏补缺：依据安全能力建设标准体系，识别出对当所缺失的关键技术、和产品，并纳入到新的技术和标准体系中，起到对所缺失产品和技术的牵引作用。

- 定义产品和技术之间的互联互通关系：识别所缺失产品和技术在能力建设标准体系中的位置，明确其与其其它产品和技术之间的关联关系，为产品和技术之间的互联互通提供依据。

建议三：制定安全运营体系标准

- 明确系统间联动的技术指标：统一安全产品间数据和指令的交互标准，实现安全产品之间的互操作，形成协同联动。

- 实现技术和管理的融合：制定安全运营模式的标准，牵引安全管理从传统的条文式、流程式管理升级为以数据驱动的新安全管理，实现安全管理流程与安全技术和运营活动紧密对接，从而有效克服软硬件的漏洞和人的不可靠性。

- 实现安全运营的服务规范性：对安全日常性工作、事件发现处置工作、应急响应工作的活动及流程建立标准，并逐步条令化，从而提升安全运营的规范性。

建议四：制定安全效果评价标准体系

口 建设效果评价

安全建设与规划的偏离度：依据标准检查安全建设是否严格按照规划内容开展。

安全建设能力体系的完成度：依据标准检查安全能力建设的完成度，使安全能力的建设的程度可以被度量。

口 运营效果评价

形成以效果为目标的评价流程和机制保障：持续对网络安全产品、技术、服务的效果进行评价，以统一的标准对网络安全能力进行查漏补缺，提升运营效果的有效性和规范性。

口 新风险跟踪评价

制定对新风险的跟踪评价体系：持续对新业态、新场景、新技术引发的网络安全风险进行评价，确保及时将相应的安全措施纳入安全防护范围。

THANKS!