疫情之下网络安全防护建设思考

邱杰

湖北省卫生计生信息中心 副主任

2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

面向未来，共护安全

——— 疫情之下网络安全防护建设思考

湖北省卫生计生信息中心
邱　杰

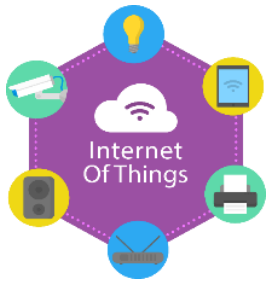
2020年8月

目录

- 网络安全形势与挑战
- 网络安全工作实践
- 困惑及思路探讨

01 网络安全形势与挑战

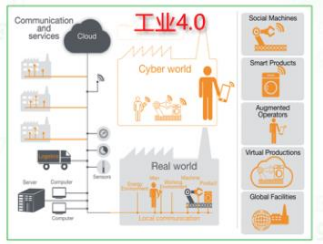
数字化转型带来了新一代信息技术加速应用



物联网
移动互联网

大数据产业
快速成熟

政府企业
迅速数据化



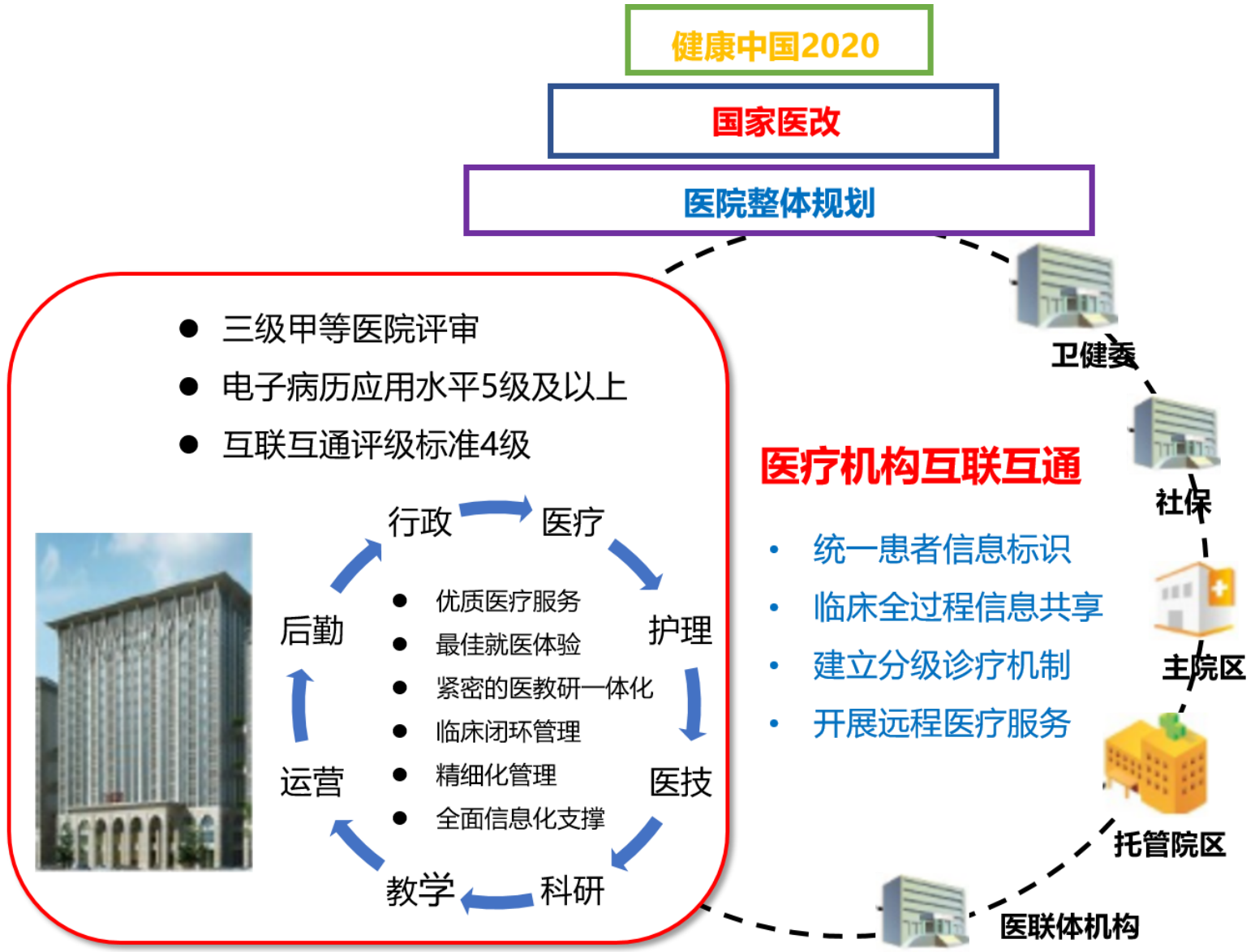
智能革命
爆发

政府决策、移动协同 、数字医疗、数字城市、智能制造、数字营销.....

医疗卫生数据跨区域、跨部门广泛共享

1. **城市医疗集团**
2. **县域医共体**
3. **跨区域专科联盟**
4. **远程医疗协作网**

医联体被列入新医改的重点举措后，全国各地医疗机构纷纷响应，2017年作为“医联体”体制框架搭建的高峰期；2018年进入加速推进期；2019年，随着分级诊疗的持续推进，各地不断夯实“医联体”建设



体制调整与业务创新带来挑战

边界泛化

- 组织边界
- 院区边界
- 系统边界
- 网络边界

资产复杂化

- 设备数量
- 设备类型
- 业务系统

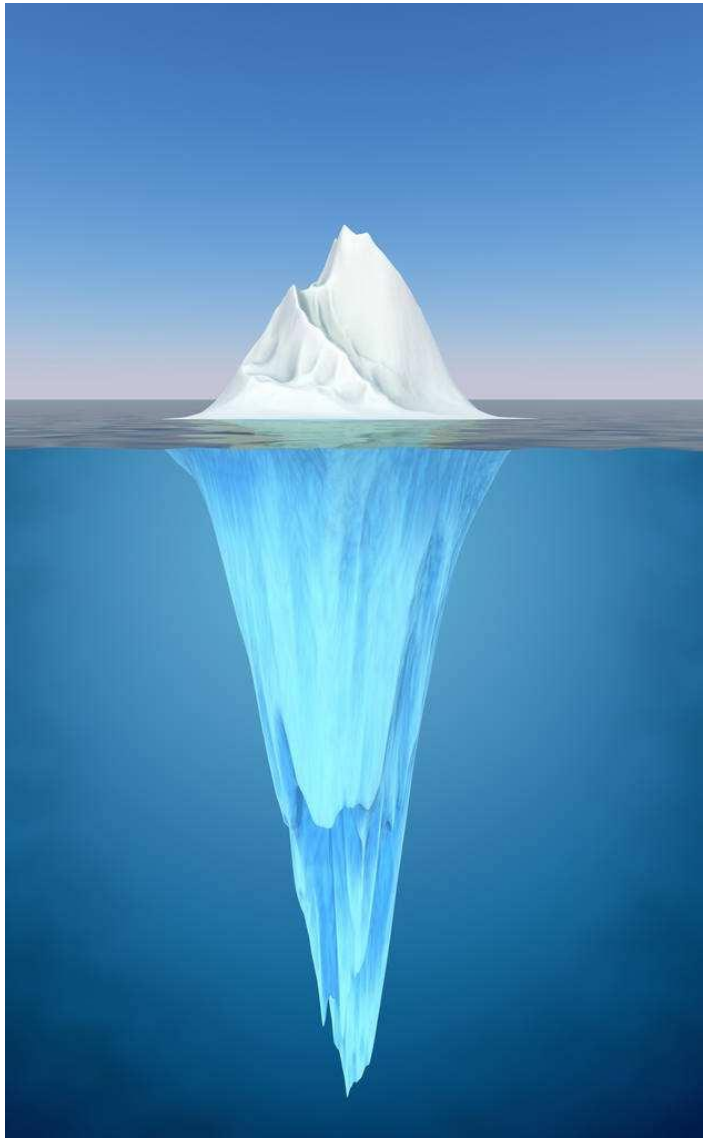
管理困难

- 安全意识
- 统筹规划
- 专业技术团队

近年来，网络安全威胁愈演愈烈

- 勒索攻击多样化
- 信息泄露愈演愈烈
- 数据集中成为核心目标
- 内部威胁防不胜防

冰山之下，风险更大



1、现有安全问题繁杂，无从下手
2、“互联网+”时代内外网边界消失如何应对
3、泛终端种类及数量众多，问题不断，运维困难
4、弱口令难以管控
5、医疗设备成为病毒的“乐园”
6、说不清的端口开放列表
7、安全建设影响安全生产
8、第三方运维人员带来一定的安全风险
9、安全培训收效甚微
10、信息部门内部安全问题
……

来源：2019BCS医疗技术论坛

02 网络安全工作实践

实践1- 建立制度，落实责任

积极响应国家政策及上级部门的要求，结合湖北省的实际情况，因地制宜的制定了相关制度与政策

制度政策

01 网络和信息安全管理制度

02 网络安全应急预案

03 关于推进网络安全等级保护工作的要求

04 平台建设及应用系统部署技术规范及网络安全要求

实践2- 培训指导，提高意识

突发事件应急指导

针对医疗单位爆发的勒索病毒等安全事件，提供应急处置方法，协调专业安全团队快速响应解决

日常监测及处置

针对全省重点医疗单位进行不间断监测，发现问题后下发《限期整改通知书》，并在限定时间后进行复查

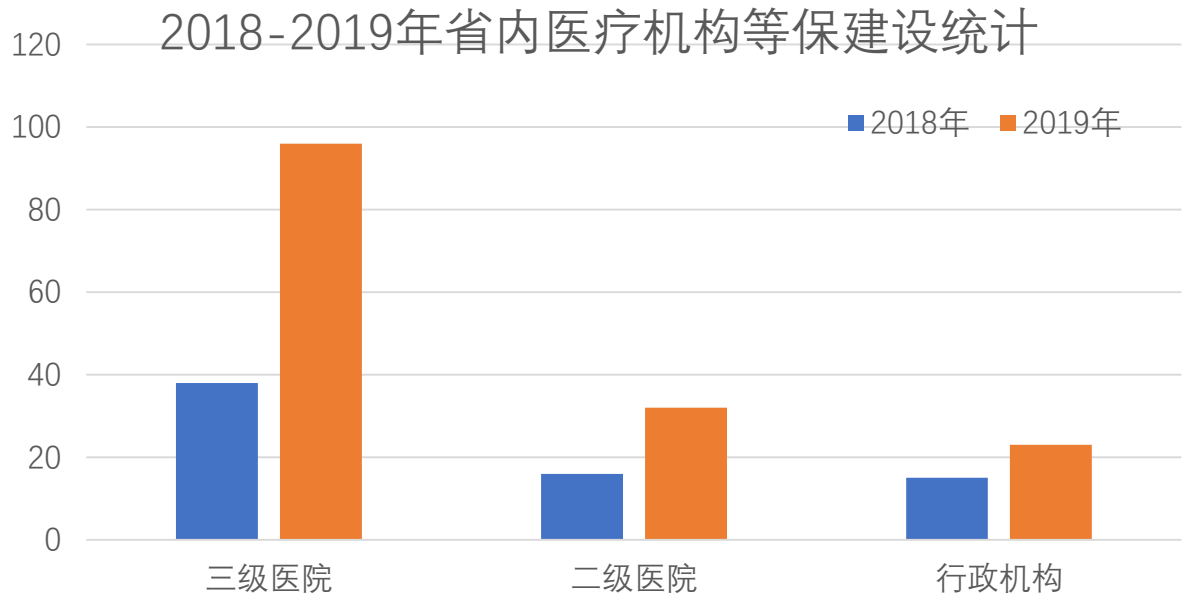
系统建设安全要求与指导

在医疗单位业务系统建设初期，对网络安全建设提出需求，做到同步规划、同步建设、同步运营

实践3- 落实等保，提升能力

等保基本情况

分类	单位数量	业务系统数量	等保三级系统数量	等保二级系统数量
三级医院	63	172	129	43
二级医院	35	70	24	46
行政机构	27	57	33	24



实践4- 多方支撑，共护安全

01

建立跨部门联动机制

与网信、公安、国家卫健委等单位建立跨部门的联动机制，相互配合，联防联控。

通报整改：网信91次
公安32次
国家卫健委34次

02

7×24小时实时持续监测

省市卫生健康委信息系统162个
重点医院业务信息系统42个
省市县医疗卫生业务系统128个
地市疾控中心业务系统16个

03

攻击防护与处置

组织专业安全厂商等社会力量共建防御体系，共拦截各类攻击500万余次，发现并阻断高危攻击IP32个，包括美国、欧洲、俄罗斯等国家和香港、台湾等地区，加强了安全防护能力

03 困惑及思路探讨

困惑与难点

困惑

难点

→ 01 **安全意识不足**

各级领导都很重视，但具体工作人员难以有效落实责任

→ 02 **安全制度不完备**

A：制度尚未细化到每一个工作人员的责任与义务，难以进行量化与考核

B：资金投入缺乏科学合理的长效机制

→ 03 **安全能力不足**

A：旧有业务系统难以应对当前的网络安全威胁

B：新的网络安全威胁与隐患层出不穷

C：符合机构自身业务需求和防护要求的厂商难以寻求

建设思路 - 提高意识

安全培训

行业内安全竞赛

指导、检测

行业内部

社会层面

网络安全宣传

网络安全会议、论坛、学习

功防演习、应急演练

建设思路- 健全制度

完善安全制度，推动落地执行

1、成立专职小组负责考核工作
2、制定网络安全量化考核细则
3、明确个人职责、义务与分工
4、确定考核周期、奖惩机制及改进方法

安全专项投入，持续建设运营

1、在信息化规划、建设及运营阶段均同步考虑网络安全投入
2、每年根据当年的安全建设及运营情况制定第二年网络安全运营计划及投入细则，审批后专款专用

建设思路- 完善机制

安全的落地实现需要新机制保障

新机制

机制保障：将信息化建设与运维工作同网络安全的防护与响应过程结合，达到工作任务事项级别的深度绑定，实现二者的**同步规划、同步建设、同步运营。**

技术聚合

为信息化发展的各个领域、各个层面注入安全基因，融入多样化的安全防护机制，实现网络安全与信息化的深度结合，并覆盖信息化环境的方方面面，实现**全面覆盖、深度结合、实战运行、协同响应。**

数据聚合

安全数据的驱动，是实现威胁感知、有效运营、协同指挥、快速响应的关键保障；**业务访问数据**对于业务运转状态、IT风险有着至关重要的作用，二者在安全实践中**互为驱动，**才能让运营变得有活力。

人的聚合

技术聚合、数据聚合归根结蒂还是要靠人的聚合：首先要保证建设运维与防护响应的**职责融合**；其次**IT技能与安全技能要实现融合。懂安全的IT人才、懂IT的安全人才**都是当下安全人才市场最为迫切的需求。

建设思路- 补全短板

基于行业实践，实现医疗行业网络安全能力迭代提升

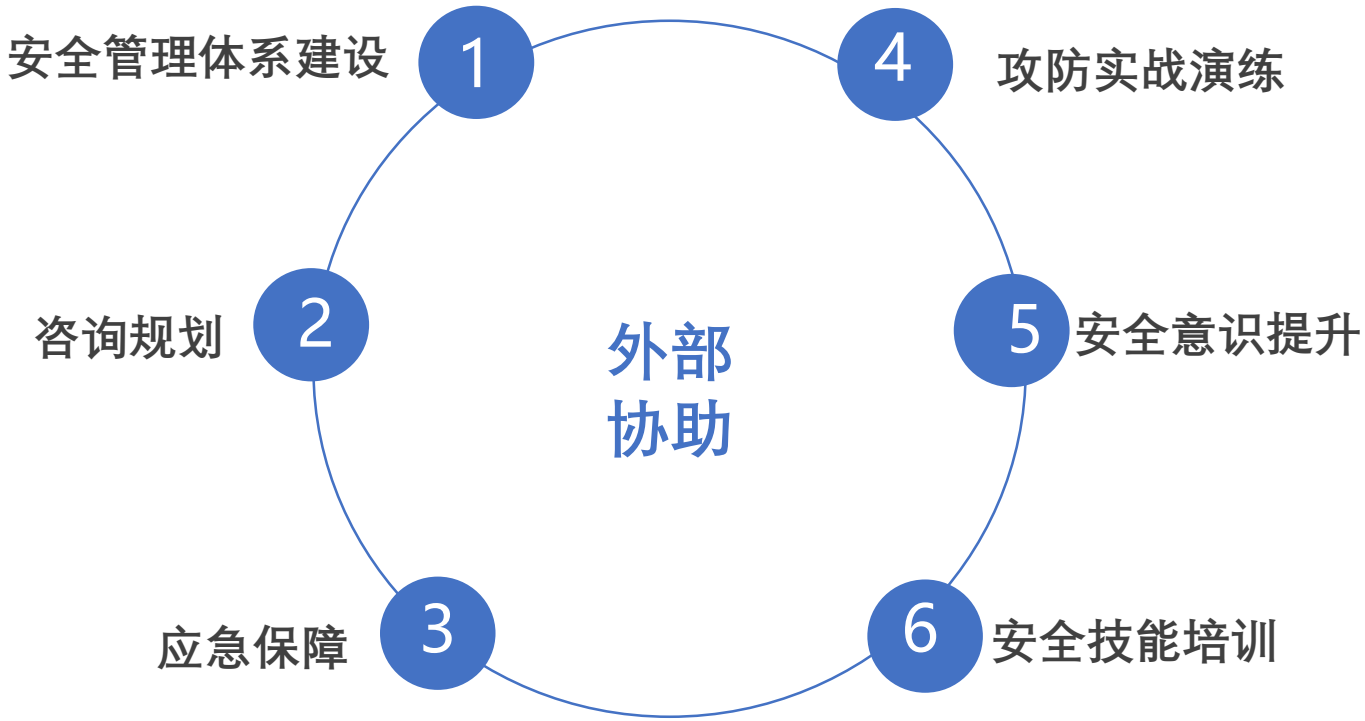
依赖 → 进化

架构安全	被动防御	积极防御	威胁情报	进攻反制
科学规划 强身健体	构筑工事 纵深防御	全面检测 快速响应	获取情报 准确预警	进攻反制 先发制人
ARCHITECTURE	PASSIVE DEFENSE	ACTIVE DEFENSE	INTELLIGENCE	OFFENSE
The planning, establishing, and upkeep of systems with security in mind	Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction	The process of analysts monitoring for, responding to, and learning from adversaries internal to the network	Collecting data, exploiting it into information, and producing Intelligence	Legal countermeasures and self-defense actions against an adversary

去病痛 → 健肢体 → 聪耳目 → 强筋骨 → 泽四方

从快速响应到自我免疫的自适应能力

建设思路- 提升能力



选择关键因素

1、能够对现状细致调研，结合未来发展趋势，因地制宜的设计整体网络安全建设运营方案

2、能够提供长期稳定优质的安全服务，解决各类安全问题并协助我方提升安全能力


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音