内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

# 网安26号院

奇安信网络安全通讯 · 安全快一步

## 成功的安全在于运营

P10

——安全运营首次全维度解析



第20期

2022 年 8 月

奇安信
新一代网络安全领军者

# 打造新一代中国特色的安全托管服务

## 时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

**两种模式**
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

**多种形态**
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

**两化融合**
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享


### 首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

### 7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

### 安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

### 安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

### 专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

# 解构安全运营的“中国模式”

网络安全作为一场永无止境的竞赛，变化速度正在加快。已持续数月的俄乌网络战给世界带来了全新启示，引发国家及城市网络安全建设理念的大转变。

俄乌冲突中， 国家与城市基础设施成为网络战的重点“打击对象”。从政府、金融、电信的相关网站与服务，到电力系统，都成为双方攻击的重点。期间已发生超过 300 多次的网络攻击事件，导致乌克兰发生卫星互联网中断及运营商全国服务中断，服务能力下降至战前 13%。此外，以破坏为目的数据擦除恶意软件成为首选网络武器，严重危害关基设施。

俄乌战争被视为世界首个全面网络战，预示着未来网络攻击将成为军事冲突的标配。这意味着城市关键信息基础设施必将在未来可能的网络战中面临高密度、高强度的网络攻击。

随着我国数字城市建设不断深入，新型网络威胁尤其是 APT 攻击、勒索病毒等层出不穷的背景下，即便堆砌再多的网络安全设备，也无法改变“盲守”、被动挨打的情况。国内很多行业客户面临网络安全防御能力不足、联防联控协调指挥能力不足、安全事件应急处置能力不足、缺乏网络安全监督管理手段、网络安全保障建设滞后等五大挑战，根本无法应对高密度、高强度的网络攻击。

为了应对安全挑战，行业客户必须走出面向静态合规检查的安全建设模式，打造实战化的安全能力。

北京冬奥会随着冬奥火炬的熄灭落下帷幕。奇安信以“零事故”交上了 2022 年北京冬奥会的网络安保答卷。结合冬奥经验和在安全运营领域多年的实践经验，奇安信以“经营安全，安全经营”为理念，为数字城市相关行业及单位设计了安全运营模式。

本期的《网安 26 号院》以俄乌冲突带来的网络安全建设理念转变为切入点，全面解构安全运营面向城市、行业客户和中小企业的不同模式，深入总结落地的实践经验，希望为用户全面展示和探讨安全运营的中国模式，共同推动安全运营驱动的安全建设。

总编辑

2022 年 8 月 1 日

CONTEN

# 目录

## 安全态势




## 网空态势



## 运营模式

TS




**奇安资讯**




《网安 26 号院》编辑部

**主办** 奇安信集团

**总　编　辑**：李建平
**副　总　编**：张　颖
**安全态势主编**：王　彪
**月度专题主编**：李建平
**攻防一线主编**：魏开元
**安全之道主编**：张少波
**奇安信人主编**：孙丽芳
**安全叨客主编**：王梦琪
**奇安资讯主编**：陈　冲
**研究报告主编**：王梦琪


奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部


索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122- L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2022 年 8 月 26 日
发行对象：奇安信集团内部




内部发行　免费赠阅

## 事件篇

全球勒索软件持续猖獗，阿根廷司法机构被迫纸笔办公，英国一水厂 IT 系统全部中断服务，网络巨头思科数 GB 敏感数据失窃，国内家电巨头美的也疑似受到攻击。

### 英国一水厂遭勒索软件攻击：IT 系统中断服务 敏感数据或泄露

据 BleepingComputer 8 月 16 日消息，英国南斯塔福德郡水务公司披露，IT 系统因网络攻击而宕机，但没有对供水造成影响。Clop 勒索软件团伙宣布对此负责，并在其勒索网站公布了南斯塔福德郡水务的部分员工数据。值得一提的是，Clop 最初似乎搞错勒索对象，在勒索公告中将受害者写成另一家大型水务公司，直到对方否认才发现认错，修正为南斯塔福德郡水务。

### 阿根廷地方司法机构遭勒索软件攻击：IT 系统全部关闭 被迫纸笔办公

据 BleepingComputer 8 月 15 日消息，南美洲国家阿根廷的科尔多瓦司法机构因勒索软件攻击而被迫关闭 IT 系统。据爆料，此次攻击是新近出现的 Play 勒索软件所为。这次攻击发生在 8 月 13 日（星期六），服务中断期间，该机构只能依靠传统纸面形式提交处理官方文件。这不是阿根廷政府机构第一次遭受勒索软件攻击。2020 年 9 月，阿根廷官方移民局遭 Netwalker 勒索软件团伙袭击，被勒索价值 400 万美元赎金。

### 超 9000 台 VNC 服务器在互联网上暴露，中国最多

据 Cyble 8 月 12 日消息，安全厂商 Cyble 的研究员发现，至少 9000 台公开暴露的 VNC（虚拟网络计算，一种远程桌面共享访问系统）服务器，无需身份验证即可访问和使用，从而使攻击者可以轻松访问内部网络。近一半暴露的实例位于中国（1555 台）和瑞典，美国、西班牙和巴西的数量紧随其后。研究员还发现，其中一些暴露的 VNC 实例用于工业控制系统。

### 美的工厂多处电脑中勒索病毒？官方称与事实不符

综合消息 8 月 11 日，有网友爆料称，美的工厂多处电脑中勒索病毒，导致所有内部系统用不了，所有文件无法打开，被勒索要求 7 天汇 1000 万美金到指定账户，还称黑客是在美的集团长达 9 天的集体年假时趁虚而入。对此，美的方面回应称：这是谣言，与事实不符。美的官方微博称，“8 月 11 日，美的集团遭受新型网络病毒攻击，少数员工电脑受到感染，公司各业务系统未受影响，经营正常进行，也没有收到勒索信息。”

## 网络巨头思科遭数据勒索：VPN 访问权限被窃取，2.8GB 数据泄露

据 BleepingComputer 8 月 10 日消息，思科官方披露，内网遭到阎罗王（音译，原名 Yanluowang）勒索软件团伙入侵，少量非敏感数据泄露，并公布了攻击过程复原。攻击者首先窃取一名员工的个人谷歌账号，通过浏览器同步的账密获得了思科内网 VPN 账号，并利用复杂语音钓鱼电话获得了该员工的二次验证码，从而进入内网实施窃密。恶意黑客声称窃取到 2.75GB 数据，约 3100 个文件，其中不少文件为保密协议、数据转储和工程图纸。

## 首批针对星链卫星网的攻击手法曝光：篡改接入终端执行任意代码

据 Wired 8 月 10 日消息，比利时鲁汶大学的安全研究员 Lennert Wouters 发现，SpaceX 旗下的星链接收终端易遭受物理访问攻击，通过一系列操作，可绕过系统保护机制，获取接收终端的代码执行权限。其将这一缺陷报告给 SpaceX 后，后者回应称，星链已通过最小授权等纵深防御建设体系来进行防护，最小化这类攻击可能造成的影响。这类攻击需要物理访问用户的终端，且仅影响当前设备，不会对星链系统的其他部分造成影响。

## 网络攻击致使英国医疗救助热线“111”发生重大中断

据 BleepingComputer 8 月 5 日消息，由于受到网络攻击影响，英国国家医疗服务体系（NHS）的 111 救助热线发生重大持续性中断。这次网络攻击袭击了 NHS 的本地托管服务提供商 Advanced，111 热线约 85% 的服务都在使用 Advanced 公司的 Adastra 客户患者管理解决方案。持续中断对英国全境都造成了影响，官方建议民众使用 111 网站来访问救助服务。

## 超 2.8 亿条公民身份信息在公有云上暴露，印度政府未予置评

据 TechCrunch 8 月 3 日消息，乌克兰安全研究员 Bob Diachenko 发现，归属微软 Azure、运行 Elasticsearch 集群服务的两个未受保护的 IP，暴露了超 2.8 亿条印度养老基金持有人的个人身份信息和其他敏感数据。具体包括婚姻状况、性别和出生日期，以及与养老基金账户有关的细节信息，如公积金编号、银行账号和就业情况等。研究员在推特上将该事件反馈给印度 CERT，不到一天，两个 IP 均得到保护。印度公积金组织对此未予置评。

## 美国联邦法院系统曝数据泄露：“广度和范围惊人”！司法部已介入调查

据 Politico 7 月 28 日消息，美国众议院司法委员会主席透露，有“三名敌对外国黑客”在 2020 年初攻击了美国法院的文件归档系统，致使“系统安全”遭到破坏。该委员会已经了解到攻击的惊人广度与波及范围，且与 2020 年底披露的 SolarWinds 攻击分属两个独立事件。司法部国家安全部门正与全国各地的司法会议和法官密切合作，希望解决这个问题。

## 乌克兰 9 家主要广播电台遭劫持，播放“总统生命垂危”消息

据 CyberScoop 7 月 21 日消息，乌克兰官员公布，有恶意黑客攻击了一家经营着 9 家主要广播电台的乌克兰公司，并传播总统泽连斯基生命垂危、已在接受重症监护的消息。遭受到攻击的公司正是乌克兰最大的广播集团 TAVR Media。当天下午，泽连斯基马上发布 Instagram 视频回应，并将此次攻击归咎于俄罗斯。自俄乌冲突爆发以来，已发生多起针对两国广播电视系统的黑客攻击。

## 漏洞篇

谷歌 Chrome 官方披露代码执行漏洞 (CVE-2022-2856)，称该漏洞已遭到在野利用，基于 Chromium 项目的软件均受影响，建议用户尽快自查更新。

### 谷歌 Chrome 浏览器代码执行漏洞安全风险通告

8 月 17 日，奇安信 CERT 监测到谷歌 Chrome 浏览器官方发布安全通告，其中包括 Chrome 代码执行漏洞 (CVE-2022-2856)，由于 Intents 对不可信输入数据的验证不足，Chrome 存在远程代码执行漏洞。攻击者可通过诱导用户打开特制页面，来利用此漏洞，配合其他漏洞可在目标系统上执行任意代码。目前，官方已监测到在野利用，鉴于此漏洞影响范围较大，建议用户尽快做好自查及防护。

### VMware vRealize Operations 多个漏洞安全风险通告

8 月 11 日，奇安信 CERT 监测到 VMware 官方发布 VMware vRealize Operations 多个漏洞安全通告，其中包括身份验证绕过漏洞 (CVE-2022-31675)、信息泄露漏洞 (CVE-2022-31674)、权限提升漏洞 (CVE-2022-31672)。这三个漏洞单独利用时影响有限，但通过组合利用可最终实现身份验证绕过，并以 ROOT 权限在目标机器上执行任意命令。目前，奇安信 CERT 已监测到这些漏洞的技术细节及 PoC 在互联网上公开。鉴于漏洞影响较大，建议用户尽快做好自查及防护。

### Linux Kernel 本地权限提升漏洞安全风险通告

7 月 22 日，奇安信 CERT 监测到 Linux Kernel 本地权限提升漏洞 (CVE-2022-34918) 的技术细节及 PoC 在互联网上公开，Linux 内核存在本地权限提升漏洞，经过身份认证的本地攻击者可以利用该漏洞将权限提升到 ROOT 权限。奇安信 CERT 已复现此漏洞，经验证，此 PoC 有效。鉴于此漏洞影响范围较大，建议用户尽快做好自查及防护。

### Oracle 多个漏洞安全风险通报

7 月 21 日，国家信息安全漏洞库（CNNVD）发布通报，Oracle 官方发布了多个安全漏洞的公告，其中 Oracle 产品本身漏洞 85 个，影响到 Oracle 产品的其他厂商漏洞 231 个。包括 Oracle PeopleSoft Enterprise PeopleTools 输入验证错误漏洞（CVE-2022-21543）、Oracle Communications Billing and Revenue Management 安全漏洞（CVE-2022-21429）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据、提升权限等。Oracle 多个产品和系统受漏洞影响。目前，Oracle 官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

## 政策篇

国内，银保监会下发文件，开展银行保险机构侵害个人信息权益乱象专项整治工作，文件列举了“侵害个人信息权益行为清单”，为目前行业最深入的整治行动；

国际上，美国白宫发布 2024 财年网络安全预算备忘录，要求各政府部门落实零信任架构，在预算中体现出对实现新的、更具弹性的安全基础态势的承诺。

国内

### 《网络安全标准实践指南——健康码防伪技术指南》公开征求意见

8 月 16 日，全国信息安全标准化技术委员会发布《网络安全标准实践指南——健康码防伪技术指南》公开征求意见。《实践指南》围绕现场扫码这一最常见场景，提出技术建议，为提升健康码技术防伪能力、提高整体安全水平提供参考。《实践指南》提出，提供方可采用的防伪技术措施包括扫码后展示脱敏个人信息、语音播报扫码内容、扫码界面有多种显著防伪和变换特征等。

### 交通运输部发布《自动驾驶汽车运输安全服务指南（试行）》（征求意见稿）

8 月 8 日，交通运输部发布《自动驾驶汽车运输安全服务指南（试行）》（征求意见稿）。征求意见稿要求，从事运输经营的自动驾驶汽车应当具备车辆运行状态记录、存储和传输功能，向运输经营者和属地交通运输主管部门及时传输相关信息。在车辆发生事故或自动驾驶功能失效时，自动记录和存储事发前至少 90 秒至事发后至少 30 秒的运行状态信息。运行状态信息至少包括：车辆基本信息、控制模式变化情况、接收的远程控制指令情况、运行状态、人机交互及车内外影像情况等。

### 银保监会开展银行保险机构侵害个人信息权益乱象专项整治工作

8 月 3 日，银保监会办公厅下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，要求各银行保险机构组织开展行业侵害个人信息权益乱象专项整治工作，推动落实《个人信息保护法》，全面梳理和排查行业内个人信息保护方面的问题和漏洞。《通知》要求，自查过程中要坚持立查立改。对短期无法整改完成的问题，要建立整改台账，明确整改措施，逐项、逐步推进。

### 市场监管总局就网络安全服务认证实施意见征求意见

7 月 21 日，市场监管总局公布《关于开展网络安全服务认证工作的实施意见（征求意见稿）》。《征求意见稿》提出，将确定并适时调整网络安全服务认证目录，组建网络安全服务认证技术委员会，从事网络安全服务认证活动的认证机构应当依法设立，具备从事网络安全服务认证活动的专业能力，并经市场监管总局征求中央网信办、公安部意见后批准取得资质等 9 项意见。

## 网信办对滴滴作出网络安全审查相关行政处罚

7 月 21 日，国家互联网信息办公室发布公告称，根据网络安全审查结论及发现的问题和线索，依法对滴滴全球股份有限公司涉嫌违法行为进行立案调查。经查实，滴滴全球股份有限公司违反《网络安全法》《数据安全法》《个人信息保护法》的违法违规行为事实清楚、证据确凿、情节严重、性质恶劣。根据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，网信办对滴滴全球股份有限公司处以人民币 80.26 亿元罚款，对滴滴全球股份有限公司董事长兼 CEO 程维、总裁柳青各处以人民币 100 万元罚款。

## 印度政府宣布撤回本国《个人数据保护法案》

8 月 3 日，印度电子和信息技术部发布通知，撤回 2019 年公布的《个人数据保护法（草案）》。被撤回法案提出了对跨境数据流动的严格监管，并提议赋予印度政府从公司获取用户数据的权力，这被视为总理莫迪对科技巨头实施更严格监管的手段之一。不过，印度并没有放弃立法。据电子和信息技术部部长透露，新的隐私法草案将在不久的将来发布，政府的目标是在 2023 年初使新草案获得批准成为法律。

## 美国白宫发布 2024 财年网络安全预算备忘录

7 月 27 日，美国白宫管理和预算办公室发布备忘录，公布了拜登政府的跨政府部门网络安全投资优先事项，并呼吁联邦民事行政部门 (FCEB) 在三个网络安全重点领域进行投资，分别是：提高政府网络的防御能力和弹性、深化关键基础设施防御方面的跨部门合作、加强数字化未来的基础。备忘录指出，联邦零信任战略定义了政府部门的优先目标，各政府部门需要在预算中体现出对实现新的、更具弹性的安全基础态势的承诺。

## 美国众议院提出《改进数字身份法案》

7 月 20 日，美国众议院监督和改革委员会投票通过了《改进数字身份法案》，该法案旨在使美国的数字身份基础设施现代化，并保护美国的个人信息免遭窃取。该法案将建立一个由联邦、州和地方领导人组成的工作组，为政府机构开发安全的方法来验证身份属性，以保护个人的隐私和安全，并在公共和私人领域支持可靠、可互操作的数字身份验证工具部门。同时，该法案指示国家标准与技术研究院（NIST）制定数字身份验证服务的新标准，重点是安全和隐私；指示国土安全部（DHS）内建立一项拨款计划，供各州升级其支持数字身份验证系统。

## 英国下议院提出《数据保护和数字信息法案》

7 月 18 日，英国下议院提交《数据保护和数字信息法案》。英国认为，目前是英国脱欧后的契机，应当把握机遇，以改变英国独立的数据法。法案对数据保护框架进行了更新，使其更利于保护国家利益，保护公民权益，减轻业务负担。通过更新，英国将进一步明确负责任的数据使用，同时保持英国数据保护的高标准。此次改革将减轻企业的负担，使企业摆脱规定性要求，并授权他们以最相称和最适当的方式保护个人数据。

奇安信

新一代网络安全领军者

# 聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。


## 国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

## 首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

## 将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

## 重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

## 专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

## 市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证

# 成功的安全在于运营

## ——安全运营首次全维度解析

# 推进城市安全运营中心建设需做到“三个坚持”

奇安信集团董事长 齐向东


当前，我国掀起数字化建设热潮，智慧城市的发展前景一片大好。网络安全是数字化建设的底板工程，智慧城市的优势要想得到充分发挥，网络安全能力必须与时俱进。

奇安信作为网络安全龙头企业，一直在努力解决智慧城市的网络安全问题，积极打造城市安全运营中心的中国模式。数字时代，网络攻击手段日新月异，只有通过安全运营，不断发现问题、改进问题，才能真正筑牢网络安全防线。奇安信从智慧城市的实际安全需求出发，制定了城市安全运营中心的理论框架、技术架构和实施策略，并先后在国内二十多个城市落地实施，效果有目共睹。

特别值得一提的是，奇安信与长沙市政府携手，树立了城市安全运营的“长沙样板”。2020 年，奇安信和长沙市政府合资成立了奇安星城公司，共同打造城市网络安全运营中心。在两年时间里，建成了跨行业、跨部门、跨区域的立体化网络安全体系；为全市政务、教育、医疗、金融等行业 550 多家单位提供安全服务；发现并协同处置事件 3000 多起，协助完成高危风险整改 1000 多次，有力保障了长沙市的数字化建设。

冬奥网络安保的全面胜利，意味着奇安信把“零事故”从不可能变成了可能，这是实力的证明。我们将继续以“零事故”为目标，深入推进城市安全运营中心建设，努力做到“三个坚持”。

第一，坚持培育统一的安全运营能力。网络安全产品部署到位，只是城市安全运营的起步阶段。如果产品单打独斗、各自为战，很难满足智慧城市复杂庞大的安全需求。为了更好地解决日益复杂的网络安全难题，我们需要把安全产品横向打通、进行有效连接。在平台化战略的支撑下，奇安信将产品需要的共性核心能力标准化，真正做到协同联动和无缝整合。比如，“大禹”平台打通了攻防、运营、监管三级态势感知，让实战化态势感知真正落地，实现统一的安全运营。

第二，坚持打造无懈可击的安全运营闭环。城市的安全运营，就好像一场无休无止的“大战”，绝不能有一刻懈怠。面对随时可能会到来的威胁和攻击，必须扩充攻击视角，把战线前移，做到第一时间预警、响应和处置。为此，奇安信研发出一站式威胁情报运营系统，从样本鉴定、多源数据研判、同源分析等方面，挖掘潜在和未知威胁，及时弥补防御弱点，形成完整的安全运营闭环。

第三，坚持用实战演练提升安全运营效果。无数的网络攻击事件说明，一旦安全防线被突破，城市会面临无法挽回的严重后果。城市的安全运营水平高不高，最终还是要看实际效果，纸上谈兵不可取。这就需要通过实战攻防演练，不断提升安全运营效果。奇安信采用分层式的攻防演练，来检验网络安全体系的有效性。分层的意思是假定外网边界层被打穿，或者内网边界层被打穿，有针对性地进行查漏补缺，让网络安全能力与日俱增。

奇安信将持续和合作伙伴一起，共同拓展新思路、拓宽新路径，为我国的智慧城市建设，贡献更加优质的城市安全运营方案。

（本文摘自：齐向东在长沙数字城市安全峰会上的演讲）

# 数字社会要体现温度、便民与安全

工信部信息通信经济专家委员会委员 王春晖

《网络安全法》《数据安全法》《个人信息保护法》是数字社会治理的三大法治基石。《网络安全法》是综合立法，包括网络安全、个人信息保护，也包括数据安全；《数据安全法》在数据安全的基础上促进数据的合法有效利用，这部法的关键词是数据安全与发展并重；《个人信息保护法》规范个人信息处理规则，保护个人敏感信息。

社会具有五维空间属性：地理空间、能力空间、有序空间、人文空间、梯度空间，数字社会是数字技术赋能的社会，其本质是以文明为特征，以增进人民福祉为目标，要体现温度、文明和包容，同样要体现便民，也要体现安全，脱离了数字社会的本质，将会成为无源之水和无本之木，不但不能给社会带来智慧，而且还可能会导致数字风险和危机。数字社会生态就是要使社会的“五维空间”更文明、更便捷、更效率、更包容、更安全。

# 数字城市网络安全运营水平亟待升级

赛迪顾问副总裁 宋宇

近些年数字城市实现了非常快速发展的态势，市场规模超过了四千亿，增速在 20% 上下。随着数字城市飞速的发展，与数字城市相关的网络安全的事件也越来越多，影响越来越广泛，危害程度越来越严峻。

2022 年 4 月，健康宝受到攻击，高铁数据泄露，整个数字城市建设过程中面临的网络安全挑战非常大。如何保证各个系统的安全运转，如何保证数据和信息的安全，越来越成为数字城市建设越来越重要的问题。从国家层面，各级政府都在不断地加大对数字城市、网络安全建设的重视力度。包括密集出台跟网络安全相关的各种政策法规，把网络安全的工作协调，包括关键信息基础设计保护和网络安全的预警、应急响应等作为工作的重点。基于调研结果，大概有接近 95% 地级市都成立了类似于网络安全领导小组的领导组织，制定了相对完备的年度网络安全的工作计划。有 35% 以上的城市出台了跟网络安全建设相关的总体方案，各个地方政府正在加大数字城市网络安全建设的重视程度。

从投入来看，数字城市方面的网络安全的投入所占比重是相对比较低的，还有很大的提升空间。数字城市的网络安全发展水平层次不齐，第三以及更往后面的梯队，跟前面的梯队还存在非常大的差距。目前中国数字城市网络安全运营的水平亟待升级。

建议建立一体化城市网络安全防控体系，通过城市安全综合防控体系的建设，对感知层、平台层、数据层及应用层做到体系化防护，保护物联网终端、网络、云平台、主机和应用等关键要素，通过威胁感知、异常检测、风险评估和态势分析等能力，对数字城市中的应用和数据提供纵深防护。

# 俄乌网络战背景下的城市网络安全建设

作者 奇安信集团副总裁 张龙

已经持续数月的俄乌网络战给世界带来全新启示，引发国家及城市网络安全建设理念的大转变。

国家、城市基础设施成为网络战的重点“打击对象”。利用网络攻击可以瘫痪对方军事指挥网络、破坏交通、能源、电力、金融等基础设施，甚至能达成不费一枪一弹赢得一场战争的目的。面对高密度、高强度的网络攻击，我国城市网络安全同样不堪一击。

2022 年北京冬奥会以“零事故”交上了网络安保答卷。作为一场网络安全“真枪实弹”综合竞技比拼的胜利，北京冬奥网络安全保障的实战经验、技术产品和模式，形成大量的冬奥遗产，对于推动我国网络空间安全保障能发挥重要作用，也会对以后全球网络空间安全保障提供可借鉴的中国经验和中国方案。

## 一、俄乌网络战态势研判：关基成为攻击重点

我们长期以来一直认为，网络攻击只是民族国家武器库的一部分，但此次俄乌军事冲突中，让我们第一次真正目睹了人类历史上首次公开、大规模的网络战威力。

网络战这种无硝烟的战争模式，给一个国家、一座城市带来的破坏，尤其对城市关键基础设施网络攻击，已经开始左右地面战争的进程、甚至影响着战局的胜败。网络攻击不仅是获取情报，而且是瘫痪对方军事指挥网络，破坏交通、能源、电力、金融等基础设施的重要武器，甚至能达成不费一枪一弹赢得一场战争的目的。

### （一）网络战早已“不宣而战”

乌克兰从局势紧张开始时，大量的政府网站就已经瘫痪了，俄罗斯政府网站随后也连续遇到麻烦。可以说，在这场军事冲突开始之前，双方的网络战就已经打响了。

乌克兰在 2022 年 1 月 14 日，70 多个政府网站也遭到了网络攻击，导致大部分网站瘫痪。根据调查显示，乌克兰的外交部、教育部、农业部、国防部等网站遭到了严重的攻击，很多重要信息遭到泄露，并且黑客嚣张的在多个网站上发布“所有乌克兰的信息已经被公开，数据信息也不可能恢复，你们做好最坏的打算吧”。2022 年 2 月 15 日，乌克兰再次遭遇到大规模网络攻击，攻击对象涉及国防部、外交部、文化部和两个最大的国有银行等至少 10 个乌克兰官方网站，攻击方式采用的是分布式拒绝服务攻击。2022 年 2 月 24 日，乌克兰国家紧急事务部门称，因为遭受网络攻击威胁，乌克兰已经切断互联网，全国境内无线和有线连接都将受限。与此同时，乌克兰多次发布网络招募令，吸引民间黑客加入，抵御和反击俄方的攻击。美国政客也借此推波助澜。

俄罗斯在 2 月 24~25 日，俄罗斯国家媒体 RT 电视台两天内有几个小时网站无法访问。2 月 26 日早上，克里姆林宫官网、俄罗斯外交部、红星电视台等多家俄罗斯网站处于不稳定状态，部分用户无法正常打开页面。

### （二）国家、城市基础设施是网络战重点“打击对象”

网络战让夺取现代战争控制权的武器不再只是枪炮和子弹，而更可能是计算机网络里流动的比特和字节。没有传统战争的血雨腥风，也没有地理空间限制，网络

能到达的地方，都可能是战场。在 2022 年 2 月 24 日，俄罗斯正式向乌克兰宣战前，乌克兰已遭受 3 个波次的大规模 DDoS 网络攻击，每个波次攻击的重点也有不同。但总体而言，军政安全、能源、金融成为主要的目标对象，通过影响政府运行、经济运行秩序等方式，警示的作用明显。正式宣战后，协同传统作战力量，根据前期网络侦查，对乌克兰数百台计算机实施数据擦除攻击。同时，DDoS 攻击造成大量乌克兰政府官方网站下线，严重干扰乌克兰政府运作，并导致民众在战争初期对政府信任度下降；数据擦除攻击导致被攻击机构的技术和服务被破坏、拒止和降级；信息战行动利用乌克兰国家内部现有的分歧，诱导乌克兰民众反政府和反西方情绪；互联网连接破坏攻击导致政府和民众通信活动受到极大影响。

## 二、面对高强度网络战，我国城市网络安全同样不堪一击

本次高密度高强度的网络攻击，乌克兰显然无力应对。我们做个假设：如果我们的大中城市遇到类似强度的网络战打击，上百个关键信息基础设施（涉及政府、金融、运营商、互联网、能源、交通等）同时发生网络安全事故，我们今天的网络安全工作模式能否应对？我们不得不相信，答案是否定的。

目前，站在整体安全的角度，我们的任何一个城市中，网络安全的能力建设都是分散的，缺乏城市级别的视角统一规划、设计、实施和运营。一旦遇到网络战，必然陷入兵力不足、各自为战的尴尬境地。当前国内城市普遍存在的一大核心问题是忽视了体现“执行效率”的实战化安全运营机制，脱离了网络安全的持续运营，再先进的安全技术产品、再完备的安全管控机制、投入再大建设的网络安全体系都无法发挥其应有的预期效果。网络安全不可能一劳永逸，因此需要一个统一的中心作为网络安全空间治理的抓手，统筹安全防护能力的部署、安全运营平台的建设、安全运营组织的架构、专业安全人才的培养，提升网络空间安全治理的效能。

## 三、从冬奥“零事故”看网络安全“中国模式”的关基保护经验

2022 年 2 月 20 日晚，北京冬奥会随着冬奥火炬的熄灭落下帷幕。奇安信兑现了自己的承诺，以“零事故”交上了 2022 年北京冬奥会的网络安保答卷，这是在面临紧张的国际局势、严峻的疫情防控、复杂的网络安全威胁情况下取得的胜利，更是一场网络安全“真枪实弹”综合竞技比拼的胜利。奥运会是国际盛会，更是实战化网络攻防竞技场，历届奥运会都遭受了网络攻击，这类攻击往往出于政治目的、经济利益、间谍活动或其他目的诉求，攻击者的背后往往具备雄厚的资源支持，具备严密的组织配合、具备强大的破坏工具，2016 年里约奥运会、2018 年平昌冬季奥运会都有非常密集的网络攻击行动，2020 年东京奥运会共遭遇约 4.5 亿次网络攻击，东京奥运会官网等网站曾瘫痪 1 小时。为做好冬奥网络安保工作，奇安信打造了全维度管控、全网络防护、全天候运行、全领域覆盖、全“兵种”协同、全线索闭环的“六全防护体系”，同时，打破了一直以来由外国网络技术公司垄断奥运网络安全保障的局面。冬奥网络安全保障的实战经验、技术产品和模式，形成大量的冬奥遗产，对于推动我国网络空间安全保障能发挥重要作用，也会对以后全球网络空间安全保障提供可借鉴的中国经验和中国方案。

一是多级多部门联动、快速响应，标准化、流程化的网络安保“中国制度”。北京冬奥组委会首创了“1+3”国家级指挥体系，中央网信办设置总指挥部，公安部、工信部、奥组委设置分指挥部架构对所有场馆和涉奥场所和设施的网络安全事件分析研判。此外，由独家网络安全赞助商制度，重大活动和关键信息基础设施网络安全保护的标准体系、运行体系的建立也属中国首创。

二是用“中国产品”建设奥运网络安保体系。以“一中心两体系”为核心的内生安全系统、“六全”网络安全保障体系等中国自主研发的网络安全产品被运用到场馆网络安全等 8 大防护工程中，12 个竞赛场馆、26 个非竞赛场馆等地的超过万台终端都被“中国产品”

所保护。

三是具有独立知识产权的“中国技术”提供关键支撑。为应对冬奥期间来自境内外的网络攻击，技术体系全部自主攻坚，即项目团队研发出基于指令执行序列检测技术的新一代安全引擎天狗，不仅能防护，还能反向追踪定位攻击者；首次应用于国家级态势感知指挥平台的大禹平台，综合解决安全防护、资产管理、数据治理等问题。首次在特大型重保活动中落地内生安全情报解决方案，实现情报生产、实时检测、分析协同、研判溯源，为网络安全提供强大支撑。

四是建设最高标准、最严要求的网络安全“中国服务”体系。在各赛事场馆信息系统进行 7x24 小时不间断的全生命周期保障，建立三道防线自查机制确保自身安全性；联合数十家中央企业，打造由 300 名网络安全专家组成的“央企网络安全救援队”，保障国家关键信息基础设施在赛期的安全运行；招募数百名“冬奥网络安全卫士”，作为冬奥会网络安全“测试员”和“情报员”，协助查找漏洞。多方合力共同打造网络安全“中国服务”新标杆。

## 四、用冬奥网络安保“中国模式”保障城市关基安全

根据乌克兰的失败教训和北京冬奥会的成功经验，结合奇安信在长沙等城市网络安全工作的实践，牢牢把握网络安全面临的新形势、新任务、新要求，坚持高标准、严要求、硬约束，加强城市运行过程中的动态、持续、有效的网络安全感知能力、管控能力，应急能力、防护能力是提升城市网络安全“免疫力”的必由之路，我们认为城市级别的网络安全工作需要建设城市网络安全运营中心，统一进行网络安全的规划、设计、建设和运营工作，才能确保城市的网络安全。主要工作内容如下。

### （一）强化领导、高效管理。

组建“数字城市网络安全领导工作组”，市领导牵头，建立全市网络安全协调推进机制，督导落实全市网络安全工作责任制，统筹全市网络安全工作部署，强化全市网络安全应急协调处置，深化各级部门、机关单位、企事业单位网络安全管控要求；打造“全层面管控、全网络防护、全领域覆盖、全周期保障、全线索闭环、全兵种协同”的“六全”网络安全防护体系。

### （二）体系建设、集约运营

建设数字城市网络安全运营中心，由一个领导厂商牵头负责，统一组织工作；搭建城市一体化安全运营组织团队。工作内容要覆盖城市中所有关键信息基础设施和对应单位的应用、网络、终端等信息化资产；构建技术、管理、运营三位一体的网络安全综合治理，形成“防御 – 检测 – 响应 – 预测”的弹性安全防护体系，保障城市网络安全健康。

### （三）统筹规划、整体管控

建设城市一级、行业二级、政企单位三级的城市三级联动网络安全应急指挥与运营中心，实现安全数据和服务资源的统一管理和调度；全面感知城市的整体网络安全运行状态、网络安全态势、对网络安全风险进行全面监测预警，为政府、公共服务、关键基础设施等业务安全运行提供一体化网络安全运营保障。功在“平时”，用在“战时”，看得到的是作战效果，看不到的是作战准备。从实战出发，统一设计和部署实战演习、平战结合，提供攻击队，模拟 APT 攻击、漏洞攻击、钓鱼攻击、内网渗透，不限定攻击路径和手段，以不采用破坏性攻击为底线，以系统提权、控制业务、获取数据为目标，评估过程模拟入侵杀伤链，深入评估北京市整体安全防护的短板。

### （四）摸清家底、心中有数

利用安全情报赋能城市安全体系，运用网络空间信

息测绘技术，摸清城市资产家底。周期性开展网络空间信息测绘，梳理智慧城市完整数字资产清单，多维度统计资产分布信息、多层次展示基本属性信息、多方位支撑资产管理分析。持续跟踪资产的数字足迹、资产的变更状态和轨迹。建立城市网络空间数字资产图谱、风险暴露面图谱，持续漏洞补丁信息研判，夯实城市安全体系基础。面向城市的信息资产，利用漏洞情报全生命周期管理方法，开展持续性技术研究与判断，强化漏洞情报采集手段、深化漏洞情报分析能力、优化漏洞情报预警机制。针对缺乏补丁、无法安装补丁的资产，研究漏洞缓解措施方法，通过最优方案修复各类信息资产漏洞，巩固资产基础安全能力。汇聚多源威胁情报数据，提升城市安全检测能力。通过多种途径收集威胁情报，运用大数据技术对威胁情报信息汇总和分析，研判得出高价值威胁情报告警。持续优化和迭代威胁情报信息，全面提升城市网络安全检测能力。

### （五）实战检验、强化防线

加强攻防对抗筑牢城市安全防线，结合常态化攻防实战手段，检验网络安全防护成效。开展城市重点行业和部门常态化网络安全检查，促使责任单位网络安全综合考核，提升责任人对网络安全重视程度，检验网络安全建设成效。定期组织责任单位实战化攻防演习和红蓝对抗，以攻击者视角检验责任单位的安全体系有效性、及时性、可靠性。增强恶意攻击对抗能力，提升安全体系处置水平。通过网络流量、告警事件的综合研判，明确网络安全威胁的攻击来源、攻击手段。采用人机结合的方式，分析、挖掘攻击链条，模拟还原网络攻击现场，辅助网络攻击事件定性。通过统一收集、集中分析的方法，对恶意攻击工具进行深度挖掘并掌握关键信息。汇总攻击手段和攻击工具的分析成果，同步至城市网络安全体系的各级责任单位，提升整体安全体系的处置水平。强化潜在攻击者的发现手段，提高网络安全预警能力。确定需重点关注的攻击者（组织）名单，持续跟踪攻击者（组织）发布的攻击动态，识别攻击者常用攻击手段和攻击工具，面向潜在高风险资产进行针对性布防，强化网络安全防控能力。针对潜在攻击者，对其网络行为全方位重点监控，利用内部生成、外部采集的情报信息，通过追踪溯源、攻击链还原手段，完善潜在攻击者的信息拼图。

### （六）智能分析、精准决策

实现智能决策提高城市安全效能，基于网络安全数据分析，辅助关键决策。采用大数据技术，对不同来源的安全数据进行针对性分析挖掘。实时掌握网络攻击情况、攻击手段、攻击目标及攻击结果，精确定位网络安全隐患、问题、风险等信息。通过持续性的数据收集与比对，形成趋势性分析结果和合理性决策判断，为决策者提供借鉴依据。构建信息共享协同能力，促进网络安全联防联控。建立城市网络安全信息共享机制，针对重大突发事件、安全事件、应急处置案例等内容，明确网络安全事件对内、对外发布规则、发布对象、发布范围、发布内容。构建安全可视化能力，展示城市网络安全态势。采用可视化技术和地理空间信息资源，实时对重保资产数据、威胁攻击数据、安全事件处理数据进行综合评估，为决策者提供实时预警展示、安全事件展示、管理评价展示、资产态势展示等多维度、多视角的内容，全方位洞察城市安全态势。

### （七）强化技能、扩充人才

加强网络安全建设资金的集约化管理与使用，提高网络安全建设投入，确保资金有效运转，推动网络安全实战化的人才建设和培养体系，推动本地区高校，建设网络安全专业学科，并于城市网络安全运营中心紧密合作，共同培养实战型人才。建设网络安全展示科普示范体验基地，利用实体场地资源广泛开展网络安全教育、公益活动，提升广大民众整体的网络安全意识和认知水平。

规划快一步

奇安信 | BEIJING 2022

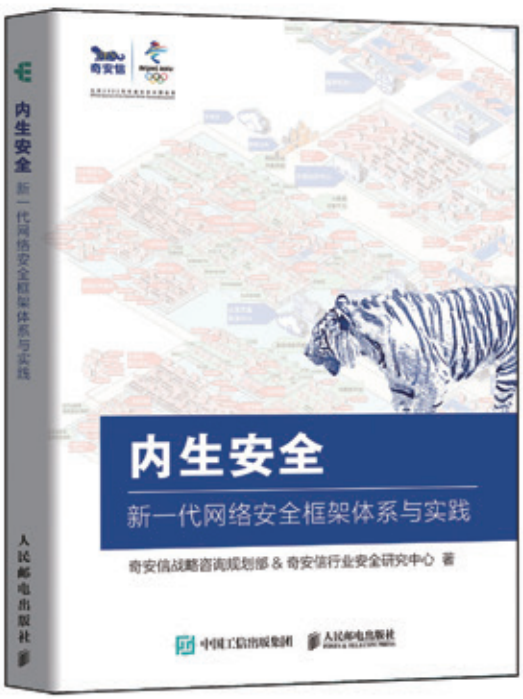
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 新书发布

## 内生安全权威解读

**19支团队、37位专家倾力打造**

**政企“十四五”网络安全规划必读书籍**




- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

**扫描二维码**
**专享内购价**

# 数字城市建设 需要网络安全深度运营的“中国模式”

作者 奇安信集团 安全运营中心总规划师 杨明洋

当前，建设数字城市已成为塑造城市发展新优势的新战略，也是建设网络强国、数字中国和智慧社会的重要抓手。“十八大”以来，党和国家高度重视发展数字经济，包括十八届中央政治局第三十六次集体学习、“十九大”报告、十九届中央政治局第二次集体学习、全国网络安全和信息化工作会议、十九届五中全会、中央经济工作会议等重要会议多次强调，要“发展数字经济、加快推动数字产业化，推动产业数字化”。

2021 年，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》发布，明确提出“加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革”。中国各地政府应加快数字化建设步伐，提升城市数字化水平。全国多地相继发布“十四五”新型智慧城市、数字政府、数字经济等发展规划，引发数字城市建设“新浪潮”。

## 数字城市建设 需要完整的网络安全架构

毫无疑问，数字城市建设已成为数字经济发展的核心场景之一。数字城市已经不是开发建设更多的信息化系统，而是推动城市的全面数字化转型，利用数字技术全方位驱动城市、赋能城市、重塑城市。这需要在顶层战略规划体系上持续完善，更需要行业和地方加快推进数字经济战略落地。

从全局性战略来看，随着我国城市基础设施建设不断完善，以及智慧城市的深入推进，使得城市发展方式发生了深刻变化，城市运行系统日益复杂，信息资源高度集中共享，安全风险也随之不断增大，“城市公共安全”“生产安全”“应急安全”“数据泄露溯源”“个人信息及隐私保护”等成为关注焦点。2015 年，公安部会同中央网信办、国家发改委、工信部共同制定出台了《关于加强智慧城市网络安全管理工作的若干意见》，要求加强智慧城市网络安全的顶层设计和协调发展，实现网络安全与智慧城市建设深度融合。2022 年，随着《网络安全法》《数据安全法》《个人信息保护法》的深入实施，城市运行安全的重要性将进一步凸显，包括生产安全、公共安全、信息安全等在内的泛城市安全将备受关注。做好与基础设施、数据资源、信息系统等相关的网络安全监测预警、应急处置及灾难恢复保障，提升应对网络安全、风险管理和运营保障的能力，将成为数字城市建设的重中之重。

从行业性落地来看，自 2016 年新型智慧城市概念提出之后，中国智慧城市建设正式有序开展，这个阶段的重点是推动大数据中心、通信网络、智慧交通等基础

设施建设；2018 年以后，智慧城市在技术上开始朝着平台化方向发展，推动城市变革原来各部门分散建设、分散管理的信息化发展模式。此外，政府推进公共服务的智慧化建设应用，智慧电力、智慧医疗、智慧交通、智慧金融等智慧应用遍地开花。2020 年新冠肺炎疫情开始蔓延，智能化、数字化手段加快赋能，城市治理水平更加高效精准。当前，我国智慧城市建设已进入全面提升的新阶段，以组织扁平化、数据共享化、业务协同化为切入点，向着集约化、融合化、一体化加速迈进。

从区域发展来看，各地纷纷加大智慧城市、数字城市的布局力度。出台了数字城市相关规划、行动计划、指导意见等，持续推动数字城市战略政策落地实施。湖南省在 2021 年 12 月 3 日通过了《 湖南省网络安全和信息化条例 》，进一步推进湖南省网络安全保障建设，促进信息化发展，以提高数字化水平，推进社会经济高质量发展，这也为数字城市网络安全建设提供了有力的支撑。2022 年，湖南省发布《 关于贯彻落实强省会战略，高质量推进新型智慧城市和数字政府建设的工作方案（ 2022-2026 年 ）》，要求以新型智慧城市建设强基础支撑，以数据资源价值释放强数字引擎，以数字产业生态培育强发展动能，以长沙高质量发展助推数字赋能等重大工程，引领带动长株潭，乃至全省数字化高质量发展，为“强省会”“强全省”贡献强劲数字力量。与此同时，长沙城市网络安全运营中心的投入与运营，也为湖南省乃至华中区域数字城市网络安全建设提供典型示范。

今年，百年变局和世纪疫情交织叠加，国际环境日趋复杂，全球产业链供应链遭受冲击，网络空间安全面临的形势持续复杂多变。此外，随着数字化、网络化进程加快，城市资产暴露面不断扩大，安全漏洞、数据泄露、网络诈骗等风险持续增加。在此背景下，数字城市建设、运营和治理等方面的工作重心也发生了重大的变化，数字城市网络安全的构建需要满足城市自身数字化转型对网络安全保障的要求。因此，需要构建一套完整的数字城市网络安全架构，为数字城市建设发展筑牢安全底座。

## 数字城市建设正面临多重网络安全挑战

数字城市建设过程中面临的网络安全挑战，主要来自以下几个层面。

首先是全球网络空间军备竞赛风险加剧，网络安全重要性凸显。近年来，全球网络空间军事竞争持续加速，强国网络军事建设已经进入从“粗放式”扩张向“精细化”纵深发展的新阶段。在关键基础设施方面，美欧以关键基础设施防护、公私和军地部门协作共享为重点，举行军民联动网络演习活动，组织军事、政府、私营机构参加，不断完善网络空间军地协同防御机制；澳大利亚政府发布《 2020 年澳大利亚网络安全战略 》，该战略的关键要素包括拟议的法律和加强的监管框架，以确保关键基础设施的安全；美国、澳大利亚、波兰等国不断调整完善国家网络安全战略，确立网络安全战略目标，并规定优先关注事项，在国家安全和军事安全全局的战略高度突出网络安全的重要性。可以预见，网络空间军事竞争的未来将是一个长期复杂的过程，现实竞争与网络空间竞争相互交织影响，将成为各国竞争的新常态。

其次是外部势力和黑客组织的严重威胁，攻击正成为常态。我国面对网络安全攻击在 2020 年和 2022 年持续增加，不仅在载体和数量方面，而且在影响方面，这些攻击往往会出于政治目的、经济利益、间谍活动或其他目的诉求，攻击者的背后往往具备雄厚的资源支持，具备严密的组织配合、具备强大的破坏工具。尤其在中美战略博弈进入近身缠斗的大背景下，我国面临的外部环境不稳定性、不确定性更加凸显，网络空间成为国家对抗的前沿领域。

最后是关键信息基础设施安全隐患严重，日益影响国家安全。关键信息基础设施作为重要的战略资源，是国家、城市、经济、社会运行的神经中枢，其安全稳定运行关系国计民生、公共利益和国家安全，日益发挥着基础性、全局性、支撑性的作用。随着国际战略格局的演变，围绕关键信息基础设施的网络攻防已成为网络空

间高烈度对抗的主战场，关键信息基础设施的安全问题已成为各国网络安全的重中之重。

数字城市建设在面临着网络安全内外重重挑战的同时，目前仍然存在着多方面的突出问题。

第一个问题是数字化转型发展和网络安全治理模式不匹配。在城市信息化实践初期，主要面临计算机病毒、网络攻击、垃圾邮件、系统漏洞、网络窃密、虚假有害信息等问题，用户通过部署各类信息安全防护手段配合运维来解决安全问题，这种静态的、被动的方式在信息化初期起到了一定的防护效果。随着信息化发展的不断深入和数字化转型发展的需要，业务系统相互作用，数据相互关联，丰富了业务场景，也使得数据在交融中赋予了更高的价值，然而国家、组织间网络安全攻防对抗形式愈演愈烈，让以往静态的、被动的方式难以满足当前数字化转型的发展，需要构建动态的、主动的新型网络安全治理模式，以应对信息化深入和数字化转型发展的需求。

第二个问题是网络安全治理机制不完善。在数字城市的发展过程中，“重视业务，轻视安全”的现象屡见不鲜，为了满足业务发展，往往在设计、开发、上线运行、业务下线等不同阶段，对业务进行补丁式的安全修补，这种“救火式”的安全介入在面对复杂的网络安全问题时显得捉襟见肘，面对复杂的网络安全形势，组织机制如何保障，安全工作如何统筹，应急机制如何运转，安全成效如何考核，这些问题如果不进行整体性考虑、系统性规划，就犹如一团乱麻，无法理清头绪。

第三个问题是业务安全需求和实际安全效果不对等。当前，生产模式向数字化模式转变，意味着网络安全防护方式发生深刻改变。安全边界瓦解，原有安全防护变得脆弱、易受攻击。政府、行业、央企等单位在网络安全建设方面大多以满足合规要求为主，安装防火墙、杀毒软件、IPS、IDS 等各类网络安全产品，配合运维工程师，保证设备正常运转，就认为网络就是安全的，近年来，有关部门和行业组织的攻防演练中，让其认识到合规仅仅是起点，而非终点。

在数字城市建设不断深入，新型网络威胁尤其是 APT 攻击、勒索病毒等层出不穷的背景下，网络安全的重要性日益凸显，即便堆砌再多的网络安全设备，也无法改变“盲守”、被动挨打的情况，仅靠安全能力难以满足数字城市建设对安全的需求。

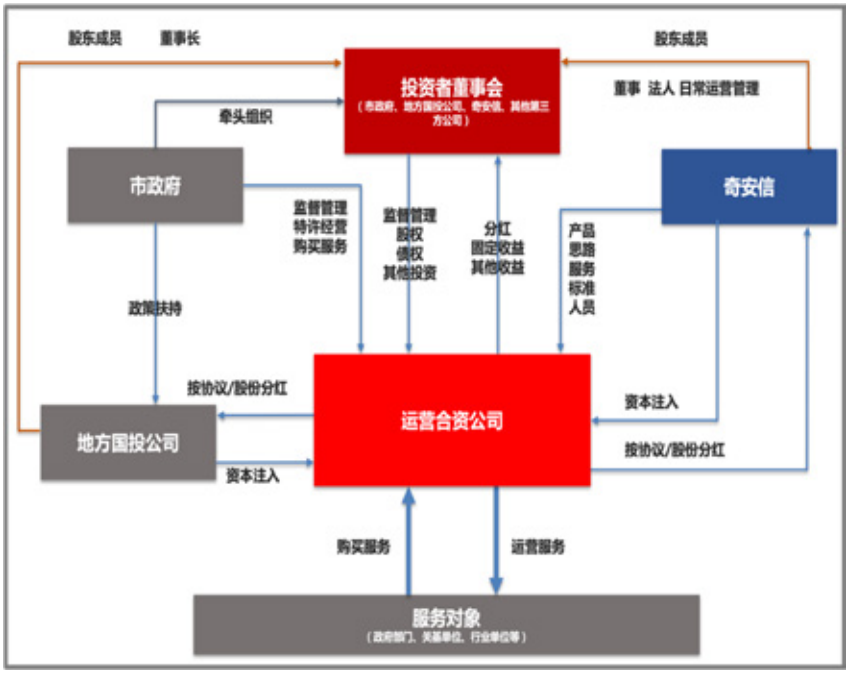
## 传承冬奥经验 三大安全运营模式为数字城市护航

2022 年 2 月 20 日晚，北京冬奥会随着冬奥火炬的熄灭落下帷幕。奇安信兑现了自己的承诺，以“零事故”交上了 2022 年北京冬奥会的网络安保答卷，这是在面临紧张的国际局势、严峻的疫情防控、复杂的网络安全威胁情况下取得的胜利，更是一场网络安全“真枪实弹”综合竞技比拼的胜利。奥运会是国际盛会，更是实战化网络攻防竞技场，历届奥运会都遭受了网络攻击，这类攻击往往会出于政治目的、经济利益、间谍活动或其他目的诉求，攻击者的背后往往具备雄厚的资源支持，具备严密的组织配合、具备强大的破坏工具，2016 年里约奥运会、2018 年平昌冬季奥运会，都有非常密集的网络攻击行动，2020 年东京奥运会共遭遇约 4.5 亿次网络攻击，东京奥运会官网等网站曾瘫痪 1 小时。为做好冬奥网络安保工作，奇安信打造了全维度管控、全网络防护、全天候运行、全领域覆盖、全“兵种”协同、全线索闭环的“六全防护体系”，真正做到了组织、流程、技术的统一。

可以说，冬奥网络安全保障是安全运营模式在应对重大活动的一次实践，充分验证了安全运营思路、模式的可行性，显示出安全运营的能力和成效，为数字城市相关行业及单位开展常态化、体系化、实战化网络安全保障工作提供了参考依据。

奇安信结合冬奥经验和在安全运营领域多年的实践经验以“经营安全，安全经营”为理念，为数字城市相关行业及单位设计了三套运营模式，让其在信息化深入和数字化转型过程中构建系统化网络安全保障体系提供一套切实可行的落地方案。

第一种模式是围绕国家战略、城市发展、产业转型，

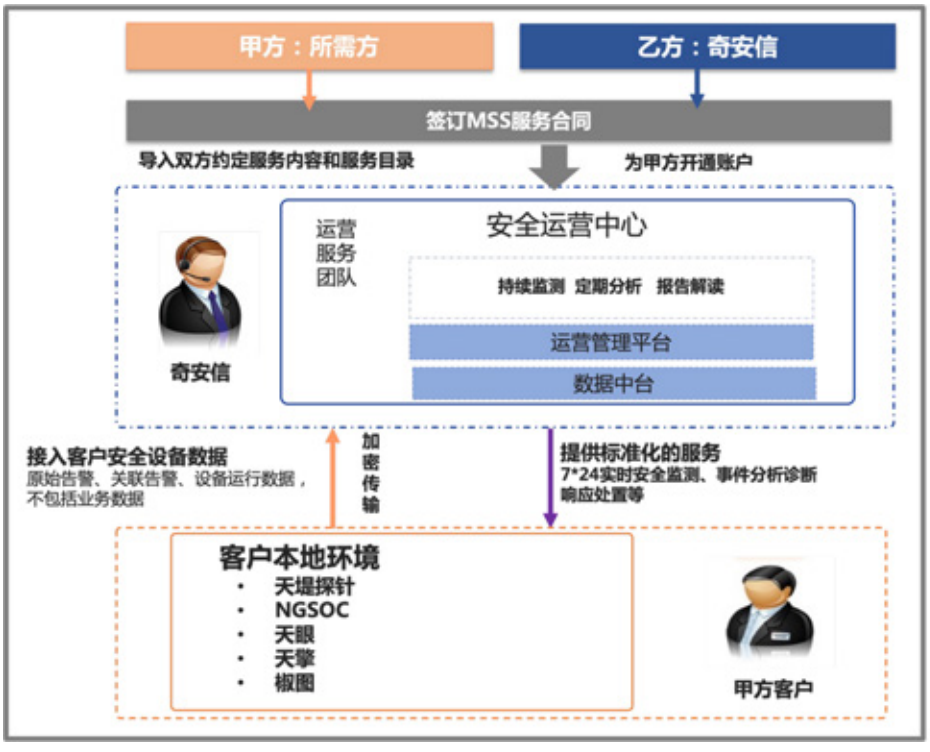



及生活方式，奇安信围绕数字城市相关主题，以城市运营中心为主体，以城市发展为目标，从实时洞察、精确感知、主动防御、联防联控、协同指挥、全城防御等方面梳理和设计城市安全运营架构体系，保障城市数字化改革的推进和发展。

第二种模式是围绕政府行业单位、央企、大型国有企业“十四五”战略目标、数字化转型中的安全需求，开展综合安全运营。

当前数字化已经成为政府、大型央企及重点行业转型发展一个重要且紧迫的问题，如何积极地进行数字化转型，又应当如何夯实政府数字化改革、经济数字化转型等重点领域的“安全底座”，开展城市多层级、协同化、整体运营。

随着各级政府积极在数字经济重点领域谋篇布局，国内各个领域的“数字化”趋势日益明显，全民上云、万物互联成为城市新的运转方式。在这样的发展趋势下，作为城市中枢的关键基础设施、政府核心部门、重要业务单位的安全越来越成为城市数字化发展关注的焦点。当前数字化正在全面重塑城市治理模式、发展模式



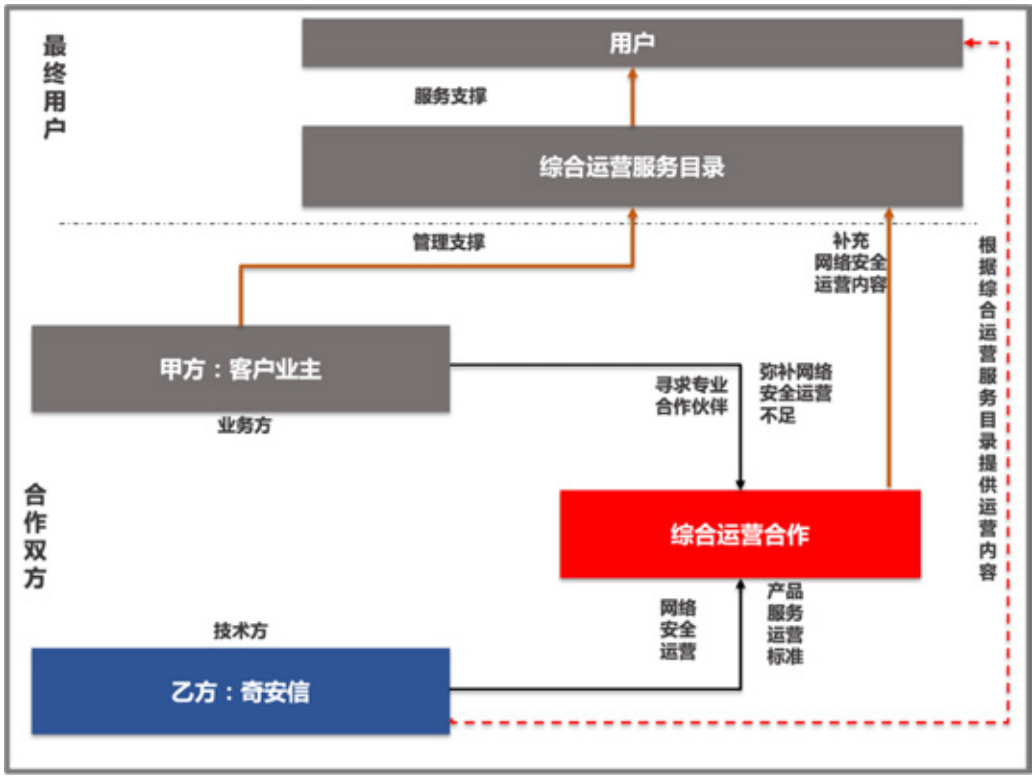
结合自身实际情况开拓出一条高效、安全、可靠的数字化之路，已成为当下许多决策者关心的重点，而网络安全在数字化进程中扮演重要的角色。奇安信面向政府、大型央企及重点行业，围绕其数字化转型发展的业务目标，与之一起相互补充相互借力，共同组建政府、大型央企及重点行业的安全运营体系，提供全方位的安全运营能力和服务，有效弥补其在网络安全技术、网络安全管理方面的不足，实现高效、持续、稳定的安全运营效果，保障政府、大型央企及重点行业数字化转型健康稳定发展。

第三种模式是为中小型企业、科技创新型企业、重点领域孵化型企业提供线上托管安全运营，解决企业在发展中的“安全顾虑”。

中小型企业、科技创新型企业、重点领域孵化型企业是带动城市高质量发展的核心动力，是一个城市未来发展的生力军，需要保护其健康稳定发展，但是这些单位还处于发展的起步阶段，安全预算有限，无法支撑自建完整的安全体系和运营体系；安全人员数量不足，面对 7x24 小时不能间断的业务，无法进行有效支撑；无安全专岗，人员缺乏安全知识和技能，无法处理日益复杂的安全问题，并且安全人员专业性不足，面对日益增长的重保、攻防演习，深感乏力，无法处理众多告警，种种困难让其难以开展常态化网络安全保障。奇安信面向中小型企业、科技创新型企业、重点领域孵化型企业，为其提供“云地结合”的托管运营服务，协助开展常态化网络安全保障工作，保护新兴战略型企业健康稳定运行，保障城市高质量发展。

## 结束语

根据国家互联网信息办公室对外的数据，从 2017 年至 2021 年，我国数字经济规模从 27 万亿元增长到超 45 万亿元，稳居世界第二。数字经济发展动能正在加速释放，数字城市迎来新的一轮建设浪潮，奇安信为数字城市相关行业及单位设计的三套运营模式，在持续实践中已经被充分验证，是适合当下国情和数字化发展现状的“中国模式”。



# 打造数字城市“安全运营中心” 筑起“城市安全磐石”

作者 奇安信集团 安全运营中心技术规划经理 杜勇

在全球数字化浪潮的巨轮驱动下，新的战略引领、新的创新发展及新的机遇挑战综合作用下，“数字城市”这一概念应运而生，成为了全球城市规划、治理、运行、发展、创新、变革的一种新的理念和模式，而网络安全作为城市发展的必要基础，对数字城市的保护性、关键性作用日益突出。在当前数字化背景下，筑牢城市网络安全防线，构建城市一体化的网络安全防护体系，建设城市级网络安全运营中心，打造“城市安全运营中心”已是时代的必然选择和要求。那么，如何才能打造好“城市安全运营中心”？围绕这个问题，下文从指导思想、规划建设等方面对此展开了详细分析。

## 整体规划：深化城市发展的“四个保障”

数字城市中的重要业务系统包括关系国家安全、城市安全、经济命脉、社会稳定的信息系统。对数字城市数字基础设施和重要业务系统的保障主要是，让其具有更强的感知能力、更高的通信处理能力和更快的响应速度，使数字城市的网络运行更加安全和高效。“城市安全运营中心”应围绕国家战略、城市整体发展目标，从数字城市网络安全战略保障、数字城市网络安全管理机制保障、数字城市网络安全技术保障和数字城市网络安全运营保障四个方面出发，考虑安全要素、落实安全责任、做好安全工作、实现整体防护，保证城市在数字化转型过程中各类基础设施和重要业务系统的正常运行。

第一，数字城市网络安全战略保障包括网络安全顶层规划、政策法规和标准规范等方面，通过该项保障来指导和约束城市数字化转型过程中安全管理与建设运营等活动。

第二，数字城市网络安全管理机制保障是数字城市协调管理、协同运作、信息融合的关键，包括组织机构设立、人才储备和宣传培训等。

第三，数字城市网络安全技术保障从城市公共基础设施安全、关键信息基础设施安全、业务系统安全、数据安全四个层次出发，通过部署多样的网络安全产品，来应对城市数字化转型过程中出现的各类安全风险。

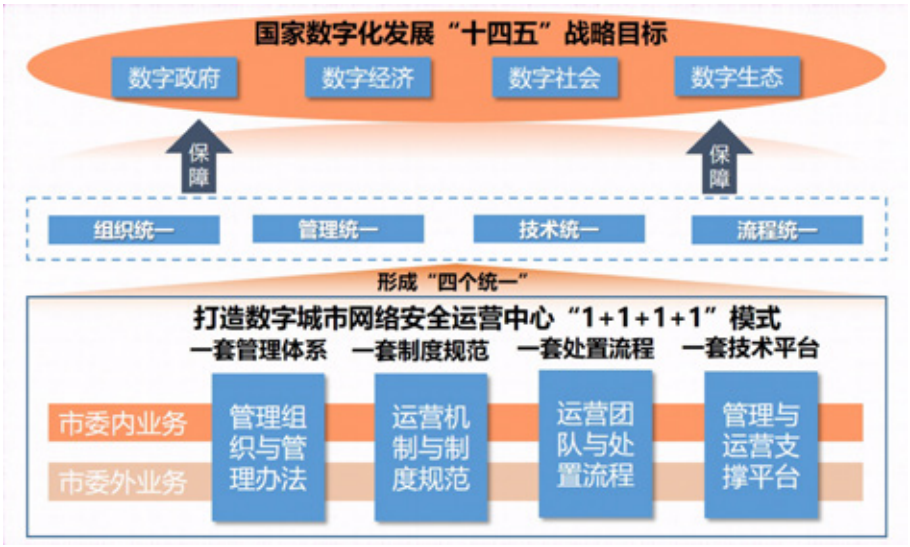
第四，数字城市网络安全运营保障是指对城市基础设施、信息资产和业务系统的监测、预警与维护。确保在城市数字化转型过程中基础设施、业务系统等状态发生变化时，可以采取一系列的预警、响应和恢复活动来保障数字城市的平稳运行。

## 指导思想：以统筹集约提升“安全效能”

“城市安全运营中心”应立足“集约赋能”推动安全能力集约化建设、集中赋能、一城通惠。一是统筹安全服务能力。让安全能力集约化、服务化、SaaS 化，形成本地化安全资源与服务目录。对全市单位进行开放，各单位可以自主化、定制化使用安全资源能力。二是统筹安全服务团队。整合市场上优秀的安全产品与优秀厂商的安全服务，将不同服务商提供的碎片化的安全服务整合成“政府主导、联合运营”的一体化安全运营服务机制。各厂商安全服务成员统一纳入安全运营中心统一服务团队，将生态服务商整合成一个有机整体，达到持续优化、动态运营的效果。三是统一安全运营服务机制，建立安全运营服务规范与标准化流程。各服务

商团队采用同一个标准参与、同一个标准考核、同一套流程开展安全运营工作。

“城市安全运营中心”并不是一种产品或者一个解决方案，是集合了政府管理、政企合作、社会资本合作、安全管理体系、平台、人才赋能等的一种新的安全运营模式。城市安全运营中心由政府牵头组建，吸纳社会资本注入，由专业安全运营公司负责平台建设、人才输出、培养和运营，可以为数字城市中的各个信息系统提供从安全咨询、安全防御、安全告警、安全处置、安全应急服务等一揽子的信息安全服务，从事前、事中、事后全面解决信息安全问题。在解决企事业单位安全问题的同时，产生一定的经济价值和社会价值。“城市安全运营中心”依托于政府资源优势，聚合社会资本和安全运营公司的能力，使三者进行有机集合。不但可以提升数字城市的信息安全水平，还可以为当地解决就业、提供税收和培养后备安全人才，从而全面提升当地的信息安全水平。目前，国内部分城市已经开始或计划建设城市级的安全运营中心，来提高数字城市的安全水平，并且国内部分安全厂商也在城市级安全运营中心的进行了资源投入。



数字城市网络安全运营总体架构图

## 建设框架：以四个统一指引“安全运营”

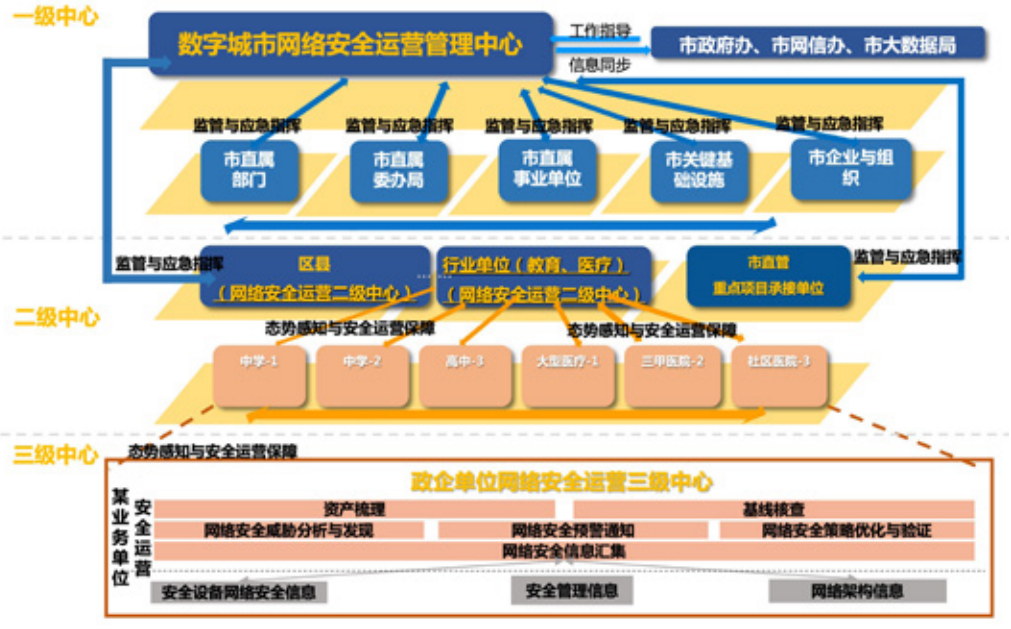
“城市安全运营中心”总体架构是通过一套管理体系、一套制度规范、一套处置流程、一套技术平台构建贯通全市委内业务和委外业务的网络安全工作机制，形成“四个统一”的效果（组织统一、管理统一、技术统一、流程统一），夯实全市整体网络安全防护体系，完善网络安全运营常态长效机制，打造数字城市网络安全管理中心“1+1+1+1”模式，实现全市网络安全业务横向到边、纵向到底，保障数字城市建设和发展行稳致远。

## 防御体系：以三级联动提升“协同高效”

面对复杂多变的网络安全形势，增强多层防御能力，构建城市一级、行业二级、政企单位三级的城市三级联动网络安全运营与指挥服务体系，实现安全数据和服务资源的统一管理和调度；全面感知城市的整体网络安全运行状态、网络安全态势、对网络安全风险进行全面监测预警，为政府、公共服务、关键基础设施等业务安全运行提供多部门、多层级协同化网络安全运营保障。与此同时，不断强化每层的防护能力及反制攻击能力。

## 全局赋能：以四横四纵筑起“动态屏障”

城市安全运营中心“四横四纵”建设以夯实全市一




数字城市安全运营“三级”联动图

全科普、典型案例宣讲为一体的网络安全宣传警示基地。

“四纵建设”通过建设“一套管理体系”“一套制度规范”“一套运营机制”“一支运营团队”四大内容，统筹全区网络安全管控治理措施，在管理、制度、机制、流程上夯实数字城市多部门、多层级、协同化的网络安全保障体系。

体化网络安全防护体系为核心目标、以“安全一件事”为服务理念，为全市各部门、各委办局 / 街道、关键基础设施、企 / 事业单位提供集约化、持续化、有效化的网络安全运营服务，提升全域、实战、动态的安全防护能力。

“四横建设”包括接入层针对数字城市政务外网、互联网、VPN、视频专网、业务应用、安全设备的流量、日志采集；支撑层以打造支撑全市网络安全业务的情报中心、网络安全中台、运营智能知识库为主要内容，即数字管理与安全运营底座；应用层由面向全市网络安全工作管理与指挥调度的安全管理与指挥调度中心，面向全市已上云的各部门、委办局 / 街道、关键基础设施的网络安全治理与运行中心，面向全市核定的需要强化重点行业单位构建行业单位安全运营中心；服务层包含产管理服务、监测分析服务、应急指挥服务、态势感知服务、安全治理服务、实战攻防服务六大网络安全服务，以及集网络安全工作成效展示、网络安

## 写在尾声

数字城市具有信息和数据高度汇集、高度融合等特点，越来越多的数据和不同的系统整合到一个平台运行，同时各个系统的关联度越来越强，承载的业务、终端、受众群体越来越多，越来越多样，与企业生产和民众生活利益息息相关，涉及企业和民众生活的方方面面，一旦漏洞被不法分子利用或入侵，产生的负面影响和后果将不可估量；另一方面，大量系统端口延伸到社区和村居等基层网点，面临着地域跨度大、业务与数字化挂钩多、网络安全建设分散单一等特点，传统的“见招拆招、头疼医头、脚疼医脚”式传统网络安全防御方式，无法应对数字时代新型的挑战，亟需建立新的安全认知及框架体系。

总体而言，没有网络安全的保障，就不可能有数字经济的健康发展，更不可能有城市的正常运行。没有坚实的数字安全屏障，就不可能有真正的数字文明时代。只有打造好数字城市安全运营中心，才能牢筑城市安全磐石。

# 综合安全运营助力企业网络安全管理能力提升

作者 奇安信集团综合安全运营业务专家 宋国利

近年来，网络安全形势变得愈加复杂。从攻击侧看，商业利益诉求和恐怖破坏目的交织，国家级攻击和网络犯罪交错，攻击呈现多样性，攻击理论和手段日臻成熟；从防护侧看，大量新技术的应用和数据的广泛流动，业务应用场景更加复杂化，安全防护的重心从基础设施为中心转向数据为中心，为政企机构的网络安全建设和运营提出了新的要求。

## 网络安全的五大问题

就目前而言，企业客户主要面临五个方面的安全问题。

第一是网络安全防御能力不足。主要体现在网络安全防御能力碎片化、协同联通能力不足，导致无法充分发挥现有安全投资的能力。

第二是联防联控协调指挥能力不足。主要体现在缺少网络安全预警信息通告平台，难以有效实时掌握基础设施的网络安全动态，导致存在大量网络攻击“后知后觉”的困境。

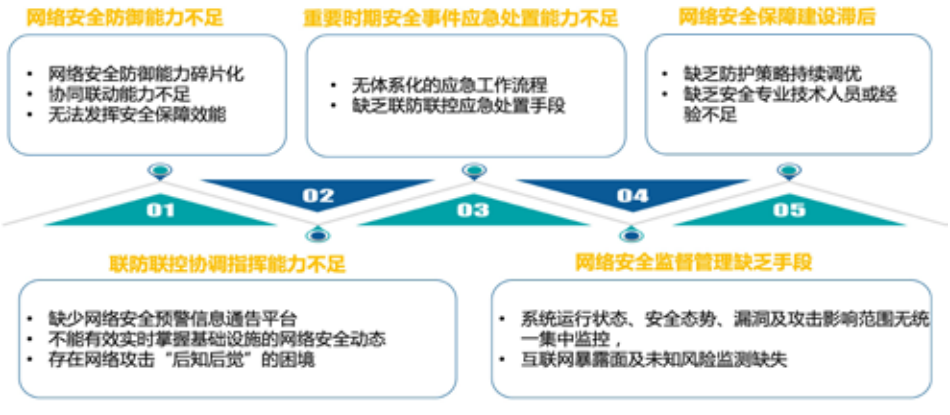
第三是重要时期安全事件应急处置能力不足。主要体现在没有体系化的应急工作流程和联防联控应急处置手段，即便能够准确、及时发现入侵行为，也难以在短时间内完成正确处置。

第四是缺乏网络安全监督管理手段，导致系统运行状态、安全态势、漏洞及攻击影响范围无统一集中监控，同时也难以监测到旗下 IT 资产在互联网的暴露面及未知风险情况。

第五是网络安全保障建设滞后，主要体现在缺乏安全专业技术人员或经验不足，导致既定的安全策略和措施执行不到位，同时防护策略也难以第一时间更新以顺应安全防御的需求。

## 走出静态合规，打造实战化安全运营能力

想要解决上述五个问题，就必须要走出面向静态合规检查的安全建设模式，并打造实战化的安全运营能力作为强有力的支持。那么究竟什么是安全运营呢？实战化的安全运营又有哪些内涵呢？




对政企机构而言，安全运营工作内容覆盖安全咨询、合规审计、渗透测试、应急响应、攻防演习、安全培训等网络安全的全流程工作，从而有效提升


网络安全质量。

奇安信对安全运营做了一个整体定义，认为安全运营对所有网络安全工作提出体系化和常态化要求，并且根据流程中的数据，分析出关键指标，进行持续提升的管理工作，主要包含现场运营与远程运营两种模式。

显而易见的是，安全运营是目标导向得，工作结果可见、可量化、可持续提升，其重点在于全量数据的采集和分析及安全流程的闭环，没有数据无法支撑量化指标，没有闭环工作就趋向形式化。

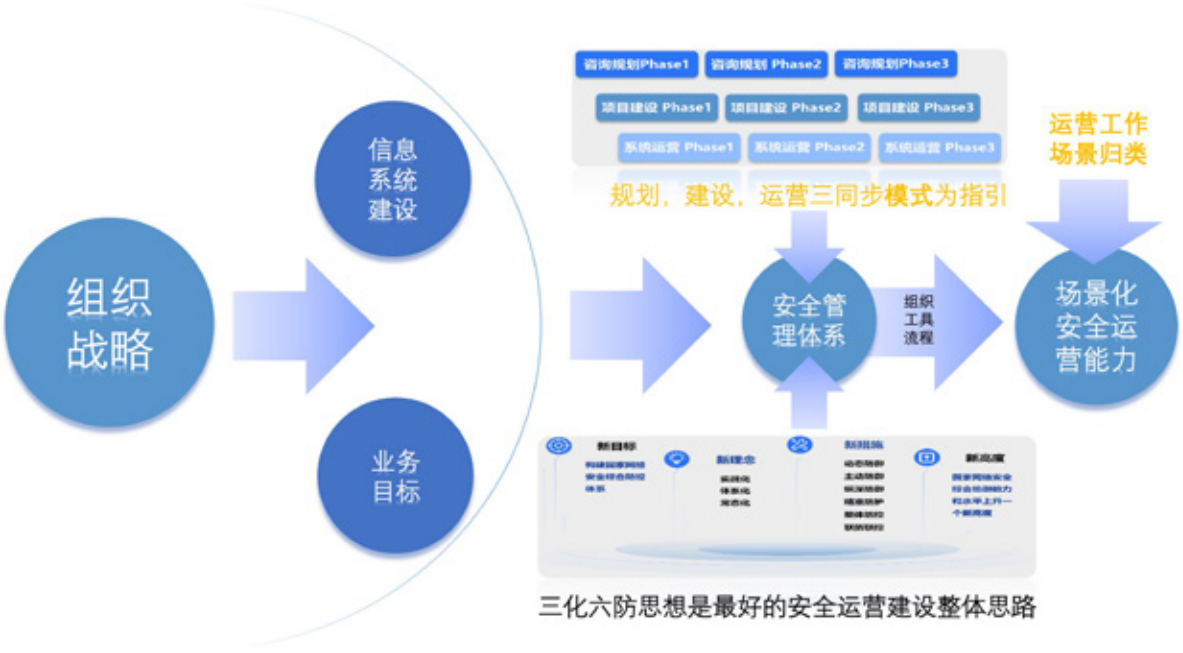
## 安全运营建设的三个前提条件

不过，想要打造实战化安全运营体系需要满足三个前提。

第一个前提条件是目标明确，要让安全能力与日俱增，保护复杂系统和复杂交易。复杂系统、复杂交易、复杂经营，三者是动态连接的。在未来很长一段时期，新技术、新应用、新场景不断涌现，因为新而且复杂，注定安全系统要不断完善，需要为安全能力设定一个能够因时而变、与日俱增的目标。

第二个前提条件是运营服务，要用专业高效的安全运营服务，来抵御复杂的网络攻击。网络安全是高度复杂的攻防对抗，攻击者会将网络攻击伪装在正常业务之中，伴随着伪装等攻击技术的进步，给安全检测带来了非常大的压力。再加上有些网络攻击者有国家背景支持，单靠政企机构自己单一的力量无法抵御这种复杂攻击，需要联动安全厂商甚至是行业上下游。

第三个前提条件是投入。安全运营的建设没有终点线，所有人都将一直在路上奔跑，因此要用足够的资源，来满足对安全无限的需求，这个资源既包括钱，也包括人。当然这也不意味着不计成本的投入，需要综合业务考量确定。



三化六防思想是最好的安全运营建设整体思路

## 满足组织发展战略的安全运营建设

有一点需要注意的是，安全的建设与业务建设紧密相关，因此网络安全必须要与企业自身业务实现全面融合和深度覆盖。

从这个角度来看，传统的网络安全建设很容易陷入两个误区：

第一是安全与业务的分离，先业务后安全，业务完成后的安全建设基本是打补丁，很多弱口令、系统漏洞问题无法彻底解决；

第二是安全项目本身设计、建设与运维割裂；三个阶段各司其职，层层衰减，最后距离最初的设想差距巨大。

想要摆脱这两个误区，就必须从模式上进行根本的创新，结合三化六防的思想，选择三同步的模式才能更好的建设安全运营能力，最终能力收束到场景。

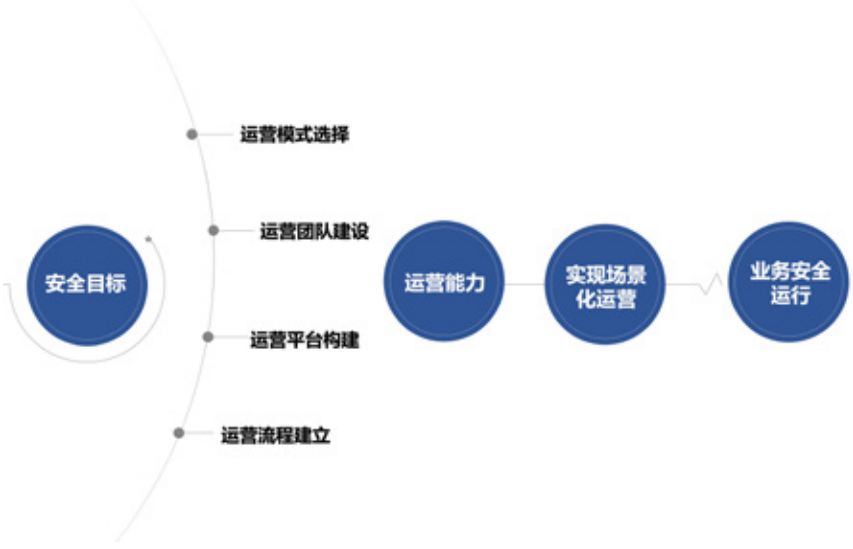
主要包含以下三点：

第一是业务建设与安全建设同步进行；第二是安全设计、建设与运营同步进行；第三是项目的各个阶段滚动前进，持续提高安全运营能力。

## 四大要素助力实战化安全运营实施

安全运营确定安全目标后，建设时需要具备一条相应的实施路径，实施路径四要素在于运营模式选择、组织团队建设、平台工具构建、流程建立。其最终的目的是建设安全运营的能力，实现场景化运营，确保业务安全运行状态。

安全服务框架有六大核心部分组成，包括运营组织建设、运营指标制定、运营流程、能力建设、实战演练、运营平台，确定运营模式与建立运营组织后，制定适合业务得运营指标，指标设定可以遵循由低到高、循序渐进的方式，过程中不断优化运营制度及运营工具，可以更好得发挥安全能力。




能力建设中，例如，资产管理服务，资产不清晰的问题困扰着每个管理员，资产管理服务可以帮助企业客户通过资产发现或监控、梳理、归档的闭环流程，帮助企业客户管理好资产。

又如，威胁分析研判与管理服务，通过监控、分析、处置、跟踪、验证、闭环流程，帮助企业用户将所接触的每条安全事件做好闭环管理，提升企业安全能力，

安全能力需要实战检验，通过渗透测试、实战攻防演练等验证模式，验证过程总结经验，持续改进才能不断提高安全整体能力。

# 安全托管服务何以成为国内政企网络安全问题的终结者?

作者 奇安信集团远程托管运营业务总监 马亮

安全托管服务（Managed Security Service, MSS），是近几年网络安全行业备受关注的领域。在我国，网络安全基础建设与环境日趋完善的大背景下，信息化、数字化水平的不断提高使得网络空间的暴露面不断扩大，恶意攻击者呈现规模化、团队化，攻击手法呈现自动化、智能化等新特征。传统的网络安全产品已不能满足客户日益增长的网络安全防护需求，安全产业结构向服务端转型成为不可逆转的趋势。

2020 年，安全托管服务市场成为全球网络安全产品与服务市场中的最大子市场，市场规模达到 271 亿美金；中国网络安全托管服务（MSS）市场在智慧城市安全运营中心和云安全等因素的多重驱动下，未来五年也将保持 30% 以上的高增速发展。

## 托管服务：形式与内容的多元

国际咨询机构 IDC 将安全托管服务（MSS）定义为安全服务提供商（MSSP）通过安全运营中心（SOCs）进行全天候监控和管理的 IT 安全服务。服务范围包括部署在本地、外部数据中心和云上的安全托管服务。国际分析机构 Frost&Sullivan 将 MSS 划分为安全资产监控 / 管理、管理威胁检测和响应（MTDR）和其他新兴 MSS 服务（管理云安全、管理 OT 安全、DDos 缓解、DNS 保护、蜜罐欺骗诱捕、Web 隔离）三类。由此可见，托管服务的形式与内容是相对多元的。

在国内，由于中国自身实际情况的特点，相对“远程托管”模式，国内更为青睐“驻场托管”模式。事实上，驻场托管也是 IDC 所定义的一种形式。目前，一些网络安全服务商均提供网络威胁检测、分析、响应、处置等多种能力，但主要为相应安全产品的增值性服务，以及提供威胁情报等。相对于国外安全产品及一揽子外包服务，国内市场普遍更为倾向于驻场托管的模式，依靠本地的安全网络安全管理平台等产品和驻场运维人员，实现对本地网络设备、网络安全设备流量和日志等的采集处理、深度分析和事件处置。在越来越多政企客户业务上云和安全分析需要依靠云计算技术实施的情况下，客户会倾向于选择以私有云方式提供服务，以更好地保障安全。

## 国内政企网络安全问题的终结者

近年来，以总体国家安全观为指导，国家网络安全工作顶层规划与总体布局不断完善，网络安全“四梁八柱”基本确立。相继出台了网络安全法、数据安全法、个人信息保护法、《关键信息基础设施安全保护条例》等网络安全法律法规，印发了《网络安全审查办法》《云计算服务安全评估办法》《汽车数据安全管理若干规定（试行）》等部门规章和规范性文件，国家网络安全工作的政策体系框架基本形成。网络安全总体工作的政策保障在快速成形，本质上是我国数字化进程的加速推进，广大人民群众对网络安全、数据安全、个人信息安全的关注度与日俱增。

在这个大背景下，网络安全工作的主体，广大政企事业单位在数字化转型发展过程中所面临的网络安全风险将会持续扩大，存在局部网络安全风险向系统性社会风险转化和蔓延的问题。另外，政企事业单位的网络安全保障体系和能力的建设，是国家安全体系和能力建设的重要组成部分。当前，政企事业单位面临的网络安全问题有以下三点：

第一，网络安全基础薄弱，短时间内难以提升，安全建设尚不成体系。目前各单位的信息化水平差异较大，网络安全防护水平参差不齐。总体来说，受制于编制、资金、意识等条件的约束，普遍网络安全水平较低，缺乏良好的网络安全基础设施，并且难以在短期内全面实现网络安全基础设施的改造升级。

第二，常态化网络安全感知和应急能力不足。网络

安全的本质是对抗，政企事业单位在攻防两端对抗中处于“能力不对等”的处境。以国家大型攻防演习活动为例，绝大多数参与企业单位在演习期间，通过加大网络安全运营人员与设备的投入，并在演习期间采取特定的应对措施，在短时间内使其网络安全防御能力得到了全方位大幅度提升。但当攻防演习活动结束后，伴随着网络安全专家和临时租借的安全防护设施离场，安全防护水平又由战时的“铜墙铁壁”回到了平时的“千疮百孔”的基础防护水平，安全感知能力和应急反应速度无法与“战时”相提并论，无法做到 24 小时全天候对安全事件进行全面准确的监测和发现，并及时开展应急处理措施。

第三，国内大部分政企事业单位还没有建成健全的网络安全体系。虽然可以跳过自建网络安全系统直接进入安全托管的阶段，但是政企事业单位缺少可以参照的行为标准和规范性的技术指导。另外，网络安全托管模式在国内缺乏“信任”的土壤，大部分政企事业单位对网络安全托管业务的认知还存在局限。可以说，安全托管服务是政企网络安全工作体系化的必经之路。安全托管服务需要更好的面对国内政企单位的特点，更有针对性的丰富我们的服务目录。

## 解读安全托管服务的模式与形态

1. 通过托管解决安全的最核心需求

在众多需求场景中，具备常态化的安全攻防检测和实战化的安全运营处置是客户最核心的诉求。为了对抗网络攻防隐蔽性强、对抗性强的特点，奇安信做了很多探索与尝试，通过云端监测响应、地端处置闭环为客户提供综合性服务；通过 7x24 的实时监测，实现常态化的安全保障；更为及时有效和准确地发现与处置 APT 事件、网络攻击事件、恶意软件事件及其他潜在安全风险；为防止疫情对安全服务造成的影响，通过视频一对一的方式与客户“面对面”沟通，提供专家深度解读、安全事件重点讲解，指导客户安全事件闭环。

2. 模式与形态

奇安信 MSS 安全托管服务的不断围绕政企客户的需求进行改进，已形成“两种模式，多种形态，两化融合”具有中国特色的安全托管服务模式。

其中，多种模式提供“直接服务、合作伙伴等紧贴客户需求的灵活的服务模式，直接服务模式是通过奇安信“MSS+”的模式，联合奇安信 NGSOC、天眼、云安全、天擎、SASE、防火墙等产品，在客户侧形成“组合拳”，奇安信实现了总部、地方的纵向联通、横向并联，构筑了整体的安全托管服务，协助客户侧建立主动防御体系的，构建管理检测和响应的进化循环。

合作伙伴模式是奇安信通过整体的技术体系、产品体系、服务体系的整合托管模式输出，形成大型企业安全运营中心、行业安全运营中心以及城市运营中心，输出能力、集约化服务。而在各类运营中心中，面向主管部门和总部机构的监管需求形成“集中服务化”，统一监测、预警与通报。各所属机构在其中存在的服务需求，可运用共享服务的理念，利用运营中心将各单位的需求进行“服务集中化”予以提供，具有服务标准统一、服务质量可控、资源高效利用等优势。

## 未来安全托管服务迎来“九化”

通过寻求专业的、可信任的合作伙伴推行网络安全托管模式，可以帮助政企单位以更小资源的投入提升企业网络安全能力，为平稳推进数字化升级转型保驾护航。另外，在业务、资金、人力等条件的受限的情况下，安全托管模式还可以快速拉齐政企事业单位的网络安全防护能力，实现各单位联防联控和信息共享。

近几年，在政策、市场需求的推动下，我们清晰地看到了中国网络安全托管服务市场的快速发展。其中，智慧城市场景下的安全运营需求和上云后的安全托管需求，直接推动了中国托管安全服务市场规模的快速增长。奇安信通过开展以支撑智慧城市为核心的城市运营中心和构建常态化和实战化的大型企业托管安全运营中心，形成 MSS 整体服务体系建设的方法论，整体输出托管安全服务能力，全面打造城市、行业、大型企业安全运营中心。为了进一步的拓展模式奇安信还在探索和运营商和大型央企的联合运营模式。

未来，安全托管服务提供商应更加注重服务工具的自动化，服务平台智能化、服务内容的标准化、服务形式的多样化、服务团队组织的体系化、服务人员的专业化、专业知识的流程化、操作流程的平台化、服务生态的规模化等内容，真正帮助用户降本增效，解决更多实际问题。安

# 安全运营之攻防演习篇

作者 奇安信安全运营专家 孙承凯

## 一、准备工作：攻防演习的本质是用实战检验动态防御能力

**问题 1：攻防演习已开展数年，合规建设已不能满足现在日趋严峻的安全风险问题，要如何应对？**

答：政企用户在安全体系的建设中以往更多在重合规、重边界、预定义的静态防御能力上下功夫，而随着全球网络安全形势的高度性不断上升、极端性快速加重，以及国内安全政策制度体系的不断完善，在“企业只保护企业安全”的需求之上，还迎来了“企业保护企业客户安全”的需求。所以这种静态能力就不再完全适应新局面，还需要形成面向过程的动态防御能力及运营水平，即持续响应、主动应变，可以理解为“静动相济，彼此赋能”。

**问题 2. 新形势下，攻防演习中如何提升自己的防御能力？需要做哪些准备工作？**

答: 实战性的攻防活动具有这么几个特点: 全网覆盖、攻击手法巧妙、强度高、应急处置要求高、时间紧迫等，为了达到预期效果，前期准备工作非常重要，在这里和大家分享一个六部曲：“定战术、盘家底、多扫雷、强意识、建渠道、要培训”。

– 定战术：确定防守战术，评估技术覆盖面，围绕重点保护部署，完善各类检测、拦截设备和工具；组织精干力量，完善管理制度和应急预案。

– 盘家底：深入排查资产，开展全方位、无死角、问题清零排查活动。淘汰老旧资产、撤销违规系统、搜索下架互联网外泄信息。

– 多扫雷：推动资产梳理，快速扫雷发现问题；全面攻击并深入路径，磨合协调响应能力；跟踪复查效果。

– 强意识：各个办公区域张贴信息安全意识口诀海报；下发社会工程攻击案例，提醒员工提高警惕主动防范；钓鱼邮件测试，帮助员工识别钓鱼。

– 建渠道：建立公开情报的收集渠道与机制，方便主动出击。

– 要培训：开展战术策略、防守场景、协同流程等机制的演练并调整优化；组织全员安全意识培训。

**问题 3. 回归到日常安全工作中，动态防御能力如何自检呢？**

答：回归到日常安全工作中，可用体系化建设为指引，构建“全场景、常态化、实战化”的安全运营能力，着力持续响应、主动应变的动态防御能力提升，同时需要建立《 安全运营成熟度与目标模型 》来判断其发展程度。我们认为，安全运营的成熟度可以分为五个阶段。

D1– 初始状态：仅仅布局基础安全设备。

D2– 基础运行：满足安全合规化建设与维护。

D3– 运行可控: 以安全能力与标准化流程构建为主。

D4– 体系运营：实现安全运营体系化建设及安全价值的输出。

D5– 深度运营：具备完善的安全运营能力及技术与管理探索。

安全运营的成熟度模型还能够帮助企业快速找到安全运营中的短板，并制定有针对性的策略，加速将安全运营融入政企业文化中，提升政企“安全竞争力”，不断健康发展。

## 二、战后能力进化：以攻防演习做自检转变，让安全运营体系能力得到进化

### 1. 如何应对攻防演习防守工作中的重要难点?

答：我们在攻防演习防守工作中存在的重要难点一般包括三个方面：

1、演练期间政企单位会投入较大人力和精力，抽调骨干人员在密集的攻击中进行高敏感度的防守，但这种情况不能长期持续。

2、对第三方接入或有连续业务往来的渠道出现的攻击行为，在应对与处置方面仍存在一定程度的短板。尤其是在与第三方如何快速建立安全协作渠道，受到了严峻的挑战和考验。

3、监控人员根据个人经验在海量告警和流量中挖掘价值信息，专业度有限、发现效率低、处置手段单一。

这些问题的客观存在，大大削弱了政企单位的安全防御能力。

面对这些问题，政企单位应该怎么办呢?

– 首先，逐步充实安全队伍力量，并进行更加精细和明确的专业分工，加大专业攻防人员的投入及培养。高效的安全团队通常包括基础研究人员、分析响应人员、高级攻防人员。攻防人员对于构建运营中心是必要的，主动地探测自己的脆弱性是很重要的自检措施。

– 第二，增强三方业务监控与合作，后续对三方合作伙伴资产进行梳理，将其接入情况纳入日常监控，并定期开展互动式实战演练，建立联合防御机制。

– 第三，持续探索大数据分析新技术和新方法，充分利用大数据技术整合各类监控数据，提升威胁发现的准确性，降低告警误报，并进一步丰富自动化、智能化的处置手段。

### 2. 实战化安全运营体系能力建设三步走

上期我们提到，日常安全工作中要以体系化建设为指引，安全运营体系能力的建设是比较复杂的，周期长在不断完善和进化的安全队伍力量能力基础之上，我们可以参考以下安全运营能力构建的三个阶段。

D1– 以资产为核心的基础防御能力：参考行业规范，夯实安全基础，建立安全管理流程、梳理并管理业务权限、应对外部各项安全检查，做到查漏补缺。

D2– 以大数据分析为核心的主动防御能力：打造安全运营平台和集中告警中心，对多种来源数据进行整合，设计告警融合、分析统计、场景建模等数字化工具助力安全监控、安全分析、威胁响应等安全运营工作，除了对安全设备本身告警，还要对应用、系统、中间件、网络乃至性能等运维监控类告警数据做融合关注，有效发现异常访问行为，做到看的清、灭的快。

D3– 以威胁情报为核心的持续对抗能力：建设威胁情报收集、生产、统一处理、0day 攻击情报、多源情报融合的情报工作机制，并结合威胁建模等威胁发现方式，可提供快速的威胁预警和告警能力，同时可与自动化封堵平台联动，助力对安全威胁的主动应对和攻击打击；努力达到未卜先知。安

# 迈向 2.0 时代
# 四位一体的数字城市安全运营长沙模式

作者 国家网络安全产业园区（长沙）城市网络安全运营中心 主任
奇安星城网络安全运营服务（长沙）有限公司 总经理 王鑫

以勒索、挖矿、APT 等为代表的新型网络攻击活动的持续活跃，引发了全球每年数以千计的重大网络安全事件，工厂停工、城市停摆的新闻屡见不鲜。数字化的城市正面临着网络安全的重重危机。

目前国际环境日趋复杂，全球产业供应链遭受冲击，网络空间安全面临的形势持续复杂多变。此外，随着数字化、网络化进程加快，城市资产暴露面不断扩大，安全漏洞、数据泄露、网络诈骗等风险持续增加。在此背景下，数字城市建设、运营和治理等方面的工作重心也发生了重大的变化，数字城市网络安全的构建需要满足城市自身数字化转型对网络安全保障的要求。

## 数字城市网络安全的五大痛点

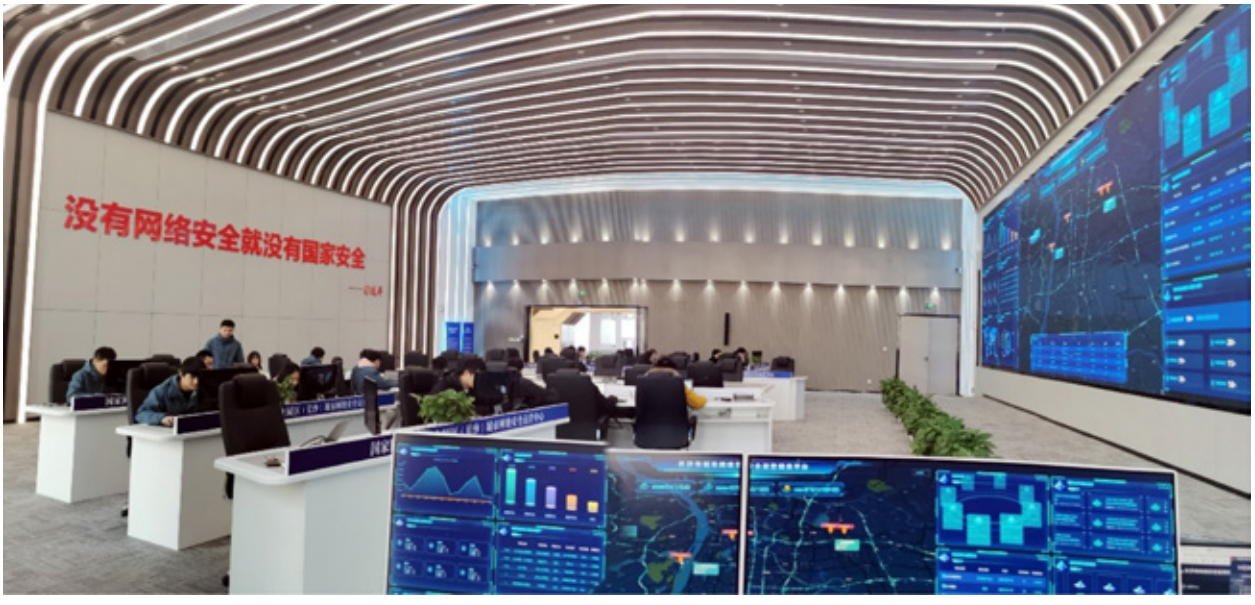
面对复杂的数字城市网络安全形势，目前主要城市网络安全存在以下五大痛点：

第一，管理制度不够完善。管理部门之间责任边界模糊，导致管理机构重叠、分散管理严重，网络安全主体责任意识不强，信息化基础资源集约建设部门承担过多的非主体安全责任。

第二，联防联控措施不足。大部分数字城市在应对日趋复杂多变的网络安全攻击形势时，缺乏统一调度，部门联动机制不健全，使整个城市网络安全管理功能难以发挥，对影响城市重要信息系统的网络安全问题处理被动滞后。

第三，监督管理抓手不强。缺乏有效技术手段的监督和评价机制，导致城市网络安全管理工作成绩无法度量，安全决策缺少科学化、精细化的数据支撑。

第四，防御能力参差不齐。缺少网络安全战略方针和规划设计，城市各单位网络安全分散建设，导致城市




国家网络安全产业园区（长沙）城市网络安全运营中心

整体网络安全建设成本高、防御能力参差不齐，在应对各种新型网络攻击时，以城市为整体的安全保障能力不足，安全事件频发。

第五，应急处置力量不足。数字城市安全运营机构兼职现象严重，缺乏实战型、技能型网络安全人才，导致网络安全管理人手不足，大量基础性的工作无法被有效执行。

考虑到上述五大问题，统筹网络安全建设、运营和管理，一定是智慧城市发展的必然要求。2020 年，长沙市人民政府与奇安信集团签订合作协议，强强联手合资成立奇安星城网络安全运营服务（长沙）有限公司，主要承接两大工作，一是长沙市新型智慧城市和数字政府网络安全保障，二是国家网络安全产业园区（长沙）城市网络安全运营中心建设运营。

为此，长沙市确立了数字城市网络安全建设的专项行动，包括初步建成全市统一的网络安全运营管理中心，全面汇集网络基础信息资源和网络安全威胁信息，建成网络安全管理平台和监测预警与指挥调度平台、可视化安全态势感知、大数据安全智能分析平台，形成统筹多领域、多层面安全监测、智能分析和应急联动的安全防护体系。建成完善分工负责、协同联动的统一安全管理工作机制，提供多层次、多维度的安全管理和服务保障。

中国开始数字城市建设十多年来，长沙第一个将数字城市网络安全能力和数字城市信息化本身画上了“等号”。

## 四位一体的数字城市安全运营新框架

城市网络安全治理应当包含四个角色，即安全监管部门，主要负责相关城市的统筹协调、安全审查、监督考核，评价改进。

行业主管部门，能够基于行业特性，实施本行业内的网络安全工作统一协调。

政企机构等主体责任部门，需要在满足网络安全政策法规和标准规范的基础上，根据自身特点构建相应网络安全保护平台或措施，并且接受安全监管。

运营中心，通过建立科学的网络安全运营体系和集约化的网络安全运营模式，全面加强城市网络安全保障体系和能力建设和数字化运营。

在此基础上，长沙已经完成了“四位一体”的城市级网络安全运营平台一期建设目标，全面覆盖市、区县（市）两级政务云（数据中心），政务外网接入单位，以及全市教育、医疗、交通、重点企业等 685 家单位的 1300 多个重点网站及 2600 多个应用系统，大数据集群规模超过 60 台，部署安全探针 122 台（套），日均接收各类原始日志数据 120 亿条，处理网络安全告警近 1000 万起。

但产品用得越多、规模越来越大，带来了巨大的工作量。包括长沙在内，湖南调研了三座城市的网络安全运营情况，仅仅告警数量均在百万级别以上。显然，这对于承担数字城市安全运营主体工作的奇安星城而言，是一个非常严峻的考验。

想要最大化发挥安全运营工程师的效能，就需要有一套标准化的工作流程。为此，奇安星城创新实践了安全运营“四化”模式，具体包括：

第一，服务线上化。服务产品、交付物标准化及项目管理线上化，替代以往人工线下维护的方式，保证服务进度和交付物可见，服务记录留痕可追溯，提升运营服务效率和质量。

第二，告警精细化。通过安全编排与自动化响应（SOAR）模块，实现自动化告警分诊， 80% 告警平台自动研判，通过降噪和运营标识规则，运营分析效率提升 70%，极大提升了人员复用能力。

第三，事件流程化。每份报告都需要通过工单审核

流转至用户服务平台，让相关单位参与工单流转和处置闭环，提升客户参与度，通过工单归档交付物，将事件闭环时间同步提升了 105%。

第四，运营集约化。基于统一的安全运营平台，完成 NGSOC、态势感知、云监测及补天告警数据统一接入，一站式对全市 685 家单位的安全事件进行实时监测运营。

## 平战结合、攻守兼备

需要注意的是，网络安全的本质是对抗，对抗就是攻防两端的较量，因此针对“平时”和“战时”的特点，奇安星城为长沙量身定做了“平战结合、攻防兼备”的数字城市安全运营能力。平时和战时穿插开展，能够大幅提升真实网络安全攻击的应急处置和安全防护能力。

平时的安全运营工作包括日常的资配漏补和告警的运营和针对既定安全缺陷的专项整治。日常运营主要以云地协同的方式，结合运营分析和基础运营团队 7x24 小时的持续运营，实现对僵尸资产、漏洞、高危端口暴露和安全事件的动态清零。

安全专项整治则是针对集中突出的安全问题进行精准识别，制定专项的解决方案，联合基础运营和应急响应团队实施定点清除，做到安全隐患的闭环处置，如弱口令、挖矿木马、勒索病毒、僵尸网络等的专项消除工作。

战时的安全保障主要包括重大活动的网络安全保障工作及重大网络安全突发事件的应急处置工作。针对重大活动和重要时期，奇安星城打造了成建制的安全重保团队，可随时应对各种类型和规模的网络安全重保任务。

针对突发网络安全事件和重大安全漏洞爆发时，奇安星城能够实现 7x24 小时的值守，支持全市的网络安全应急响应和溯源。

除了支持长沙市的网络安全运营工作，奇安星城还利用自身白帽子在漏洞挖掘方面的优势，向上级主管单位报送了超过三百个原创漏洞，对消除相应安全隐患做出了积极的贡献。

## 迈向数字城市安全运营 2.0 时代

截至目前，奇安星城已持续运营一年零八个月。这一年多来，数字城市安全运营的场景聚焦于互联网出口、云数据中心、网站等网络流量，主要以监测、预警、分析、研判和督促整改为主，同时帮助长沙各级政府、企事业单位制定一些相应的网络安全规章制度、管理办法。但是随着国家“十四五”信息化的重大工程逐渐深入，安全运营场景也在不断发生变化，现有的以网络安全监测为核心的城市安全运营 1.0，需要逐渐迈入 2.0 时代，把安全工作深入地切入到各行各业的信息化业务当中去，着力深化业务安全防护能力。

2.0 时代是以数据安全作为驱动，把数据整体切入到业务应用当中，所有运营工作都需要以智能化城市安全中枢平台为基础。

恰在此时，奇安信正式发布了“星城 – 城市网络安全运营平台 2.0”，能够基于安全中台安全网关，构建起覆盖整个城市的安全中枢网络，基于分布式的系统架构和奇安信自研的大数据相关技术，完成城市级海量数据的实时计算和分析。

基于星城 2.0，长沙数字城市网络安全运营 2.0 时代的工作将进一步贴合国家“十四五”信息化规划的重点业务改革方向，重点深化以下四个业务场景下的网络安全：

第一是保障高效协同的数字政府，确保政务数据共享流通安全，保障“一网通办”“跨城联办”“一网统管”等业务安全。

第二是服务共享共治的数字社会，保障基于数据的“应急管理”“社会治理”“新型智慧城市”的安全。

第三是保障普惠便捷的数字民生，保障“一卡通”“数字医疗”“数字教育”“数字文旅”“数字社保”等公共服务安全。

第四是服务数字化转型的数字经济，深化工业互联网、车联网、5G 创新发展的安全保障。

# 确立目标方向 直接关乎企业网络安全运营的成败

## ——揭秘广电运通网络安全运营的探索实践

**被采访人** 广电运通高级副总经理、运通奇安董事长 李学军
**采访人** 研究员 张少波

“企业无论规模大小，在网络安全运营中，总会面临着人员和安全技能缺乏、经费不足，工具和流程不足等问题，但这些都可以逐步解决。网络安全运营的成败，关键在于企业必须确立一个清晰的目标和方向，否则，就会头疼医头、脚疼医脚，缺乏全局全域的思考。”广电运通高级副总经理、运通奇安董事长李学军在谈及企业在网络安全运营的探索中，反复强调了确立目标的重要意义。

广电运通创立于 1999 年，是一家成立了 23 年的国有控股高科技上市企业，连续 14 年在金融智能终端市场占有率居全国第一、世界前三。近年来，广电运通加速从金融终端制造向人工智能方向转型，已发展成为国内知名的行业人工智能解决方案提供商。

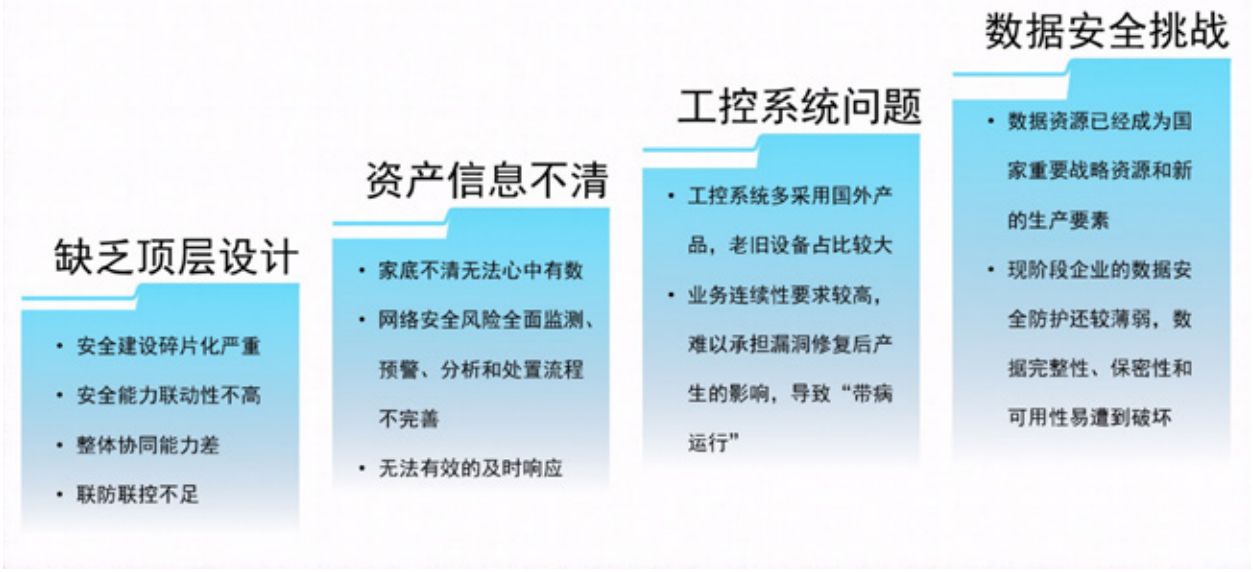
图：广电运通高级副总经理、运通奇安董事长李学军

在数字化转型全面展开、黑客攻击日益严峻、网络安全需求激增的形势下，2021 年 12 月，广电运通联合奇安信集团等合作伙伴，共同出资设立广东运通奇安科技有限公司。作为运通奇安的董事长，李学军对于企业数字化转型背景下网络安全保障工作，具有广泛实践和深刻领悟。

### 企业网络安全面临多重挑战 “目标缺失”是深层原因

李学军认为，企业数字化转型是一项同时具有长期性、复杂性、系统性的工作，需夯实四个转型基础：技术基础、管理基础、数字基础及安全基础，其中安全是发展的前提。目前企业数字化转型过程中主要暴露的网络安全问题有四个方面，分别是缺乏顶层设计、资产信息不清、工控系统问题、数据安全挑战等。

“从更深层次的角度来看，造成这些原因主要来自三个方面，排第一位的就是企业安全建设目标缺失。没有目标、没有方向，表现最常见的就是传统的头疼医头、脚疼医脚，只解决眼前紧迫问题，在建设过程中缺乏全局、全域的思考。”




“目标缺失的背后其实是认知不够”。李学军谈到，总书记说过“安全是发展的前提”，然而很多人并没有领会到这方面的精髓，如果管理层停留在传统认知的话，那么企业数字化转型也不会重视安全运营的方案建设。

第二个原因是“重业务轻安全”。目前来看，企业数字化转型的关注点仍然在业务，安全建设工作并未引起足够的重视，从而导致没有投入足够的资源来满足业务发展对安全的需求。

第三是对安全队伍能力建设未予以足够重视。RSAC 2020 的主题是“人是安全要素”（“Human Element”），全球范围都充分意识到人在网络安全中的关键作用。然而国内企业的现实是，“专业安全人才请不起，也不愿意培养”。

在很多人的意识里，桌面运维和网络运维人员兼职安全人员，以及“一人安全团队”的现象，仅仅存在于中小企业，但事实并非如此，即便是规模较大的企业，或者管理权限和范围很大的单位，安全人员短缺的情况也非常严重。李学军分享了一个真实的例子。“我们遇到某个主管单位，该单位所管辖的企业数量众多，资产相当庞大，本应具备一支专业的安全团队。但真实情况却是该单位的安全支出仅有 20 万，请一个专业的安全人员驻场服务都不够。这样导致的结果就是：下辖单位频频遭遇到勒索攻击、恶意软件入侵、数据泄露等安全事件，甚至被主管部门多次通报。然而，由于安全人员不足，该单位只能将责任往下传递，由下辖企业自行处置，再遇到类似安全攻击时也只能重蹈覆辙。”

基于大量的企业案例分析研究，结合实际建设过程中的问题，广电运通探索总结出“四个保障，一个持续”，其核心是与业界优秀的企业或成熟的安全标准进行对标，通过选取关键任务定下关键指标，并将循环运转起来，以达到持续提升效果达成指标的目标。持续提升需要涉及指标对标、安全规划、安全建设、定期演练、评估整改等。

“在整个过程中，最难的是结合现状，选取指标进行对标的环节，而后续的环节都是对前期方向选择正确性与否的验证，方向错了，或者好高骛远、不切实际，后面的环节再努力也难以达成效果。” 李学军表示。

## 推动安全运营 将问题处理渗透到“肌肉记忆”

对于大多数企业来说，“四个保障，一个持续”要

进行落地，离不开建立完善的企业安全运营机制。

企业安全运营为何有如此大的价值，李学军讲了一个形象的例子：我们知道飞机驾驶员都有一个飞行手册，在飞机起飞前的准备过程中，机长和副机长都会拿着一份 Checklist 逐项进行打勾确认。平时训练中，也会有一套标准化的 SOP 流程，将飞行中可能遇到的安全问题的处理流程要点规范化，并进行持续演练，确保烂熟于心。当问题出现时，所有操作都在电光火石间完成，以最快的方式解决问题，无需更多时间去思考讨论。

企业网络安全运营工作和飞机驾驶的复杂程度不可比拟，但他们有一个共同点，就是都需要将解决问题的流程规范化、最简化，形成所谓的“肌肉记忆”，这才能在最短的时间内解决问题。当出现新的问题和新的解决办法时，及时将它补充进流程和知识库中去，从而形成“正向循环”，不断帮助企业从流程化、规范化的角度，推进安全工作的落地。

其次，就是网络安全运营可以显著提升安全工作的工程化能力。举个例子，企业内很多有经验的安全工程师，能够对怀疑一台服务器被黑进行排查溯源，查看服务器进程和各种日志记录，然而这是工程师的个人能力，背后是深厚的专业技术和经验积累，是极其难以被复制的。

通过安全运营，企业可以借助相应的平台工具，将安全工程师的这种能力转变成自动化的安全监测能力，并通过安全平台进行应急响应和处理，让不具备这种能力的安全人员也能成为对抗攻击者的力量，这是开展网络安全运营工作带来的另一收益，将工程师的经验沉淀为组织的知识，真正实现复用。

## 企业开展网络安全运营 从“补短板”开始

很多企业深知网络安全运营的巨大价值，然而这项工作看起来千丝万缕，甚至剪不断、理还乱，导致企业不知道该从何入手。对此，李学军基于长期的实践，给出的破解之道是“先补短板”，即从最容易受到安全威胁的薄弱环节入手来开展网络安全运营工作。

“以广电运通为例，作为智能金融终端提供商、轨道交通智能设备提供商，我们会和很多供应链环节中上下游的伙伴打交道，安全的很大威胁就是来自于攻击者利用我们和供应商、代理商、软件合作伙伴之间的信任关系，通过钓鱼邮件或软件合作伙伴的开源软件漏洞，开展长期潜伏的 APT 攻击。由于防御战线被拉的很长，很难避免某个环节存在疏漏，导致攻击者乘虚而入。”

为此，广电运通的具体实践之路是，通过和奇安信这样的专业安全运营托管服务提供商合作，分步骤来补齐短板。

第一步，通过部署能有效应对此类安全威胁的安全产品和工具，开展长期的监测和动态预防，对相关数据进行定期分析和研判，及时发现并清除威胁。

第二步，不定期开展模拟的钓鱼邮件渗透演练，将中招结果和影响内部公布，并与各部门负责人的关键绩效指标挂钩，从而提升全员网络信息安全的主动意识。

第三步，通过培养锻炼企业自己的安全运营队伍，并对标企业安全工作成熟度标准，争取在 2 年内通过国内企业级数据安全成熟度最高级认证。“因为核心的数据安全责任还是得自己的队伍来负责，不能认为有了合作的网络安全运营托管公司合作自己就可以高枕无忧。”

在这个过程中，广电运通和奇安信实现了很好的优势互补。其中，广电运通在数字化转型方面走在了同行前列，对网络安全高度重视，为安全运营提供了广泛而丰富的场景实践。而奇安信拥有强大的安全智库，以及网络安全态势感知能力，它不仅仅是安全产品的提供商，也拥有相当先进的安全理念，并且在国内率先落地实践，从实践层面引领数字化转型时代的网络安全体系建设。

李学军认为，奇安信所倡导的“内生安全”“零信任”，以及基于冬奥网络安全保障总结出的“有事件 无事故”理念，具有相当的技术前瞻性，在广电运通推进企业数字化转型过程中，提供了公司总部及下属企业整体安全运营水平提升的规划思路指导，发挥了参谋作用。所有这些，都是广电运通和奇安信合作越来越紧密的重要原因。

# 安全托管服务（MSS）：人员与能力不足下的最佳选择

作者 武汉大学信息中心副主任 蔡利军

对有重要科研机构和实验室的国内高校而言，情报库更新及时的网络威胁感知系统必不可少。2017 年，武汉大学部署了基于大数据的网络威胁感知系统“天眼”，当时就发现了境外 IP 对校内敏感科研机构的窃密木马。2018 年，“珞珈一号”卫星发射期间，“天眼”也检测到大量境外黑客组织对遥感实验室的 APT 攻击。

在部署天眼之后，我们依托天眼对武汉大学校园网开展了网络安全治理；同时，利用自动化编排系统对天眼的威胁告警和边界防火墙进行联动。作为 PDR 安全模型里面的检测设备，天眼在武汉大学网络安全防护体系里发挥着重要的作用。

目前，奇安信又提供了安全托管服务（MSS），该服务能够通过微信及时通报网络安全事件，比如，我们要求 MSS 客服对 APT 攻击、Web 攻击第一时间进行告警；同时提供人工筛查网站和系统的管理弱密码服务。

目前，在高校安全人员普遍不足、安全能力缺乏的环境下，奇安信安全托管服务提供了一套完整可行的解决方案，能够提高网络安全保障工作的效率。

随着《数据保护法》《个人信息保护法》的实施，高校对数据安全的关注持续提升，我们建议“天眼”增加敏感数据（身份证号、手机号等）的检测，对异常时间和地点的敏感数据外泄通过安全托管服务进行告警，在高校数据安全防护工作中发挥更重要的作用。安

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022


# 实力晋级！

## 国内唯一大型供应商

奇安信MSS上榜Forrester亚太地区托管安全服务报告

《The Managed Security Services Landscape In Asia Pacific, Q3 2022》

- 常态化的安全攻防监测
- 实战化的安全运营处置能力
- 体系化的安全保障建设

# 城市让生活更美好，我们让城市更安全

## ——走近奇安信副总裁、区域发展中心负责人张龙

作者 公关部 孙丽芳

8 月初，北京暑意正盛，奇安信集团副总裁、区域发展中心负责人张龙打算趁热打铁，把几个在谈的城市安全运营中心集中往前推进。就在几天前，基于 MSS（安全托管）服务和市场规模，奇安信作为国内唯一一家大型供应商，入选了国际权威咨询机构 Forrester 发布的《The Managed Security Services Landscape In Asia Pacific, Q3 2022》报告。而去年，奇安信 MSS 还只是中型供应商梯队。短短一年时间，奇安信 MSS 凭借发展规模和增长速度跻身亚太地区头部供应商梯队，其综合实力获得了国际认可。

这一年发生了什么？一切还是要先从奇安信 MSS 的带头人张龙说起。

### 审时度势 迈入安全圈

张龙，1997 年大学毕业，通信专业。毕业后先到西门子 IT 部门工作，后来转岗到售前和产品经理岗位，主攻网络工程，2005 年跳槽到美国公司 Juniper Networks。Juniper Networks 当时收购了全球硬件防火墙的老大 Netscreen，张龙就此开始接触安全圈。

“我那时候做系统工程师，这个岗位是什么概念呢？就是客户侧所有的问题你都要管，不管是售前、售后、还是测试，你是唯一的接口人。那时大家对安全的概念仅仅存在于要有防火墙，要有入侵防御，要有防病毒，但都是一个个的单点，体系化的技术知识基本上靠自学。这件事我干到了 2012 年。”

15 年的时光，张龙在网络工程领域已经干得顺风顺水，但是他却在此时感到了危机。

“当时我在反思两件事情，第一件事情是网络工程

到了 2012 年就已经很成熟，成熟到大学毕业三四年的工程师和我们这些已经干了十多年的工程师，在做一个工程设计和实施的时候，会发现大家是雷同的，我们只是经验更丰富一点，但其工程化标准已经很完善，所以我觉得网络工程这条路可能不太能走下去了。还有一件事情是我们当时看美国的安全市场，已经一半是服务，一半是产品，而中国的安全市场却还是在卖盒子。我跟客户沟通网络安全工作的时候，客户中水平比较高的人已经认识到这一点，说你们卖的这些东西解决不了我的问题。那时候我就开始设想 SoC（网络安全运营中心）该怎么建。我们一群工程师也总在一块讨论，一方面是讨论我们自己的未来。另一方面，也是基于这个话题，我们在选择自己下一步的技术方向。”

当时摆在张龙这群人面前的技术方向有两个。一个是云计算方向，因为当时所有做网络的人都懂 SDN、虚拟网络。另一个就是安全方向。

工程师的谨慎思维让张龙选择了后者。“作为工程师，我们有时候思维偏谨慎，当时觉得云计算的商业模式看不懂，但是安全怎么赚钱，大概看懂了，而且我们发现安全这个领域，你的工作经验是有附加价值的。安全的标准化很差，它更多依赖于有经验的人处理复杂局面。安全本质上就是一只手是管理，一只手是技术。”2014 年年底，张龙加盟了刚刚成立的奇安信，真正进入了安全圈。

虽然换了赛道，张龙的优势却很明显。“网络技术功底帮了我很多忙，因为工作中很多时候，我们要跟网络运维和云计算的人打交道。后来在一些大型项目里面，我还会邀请一些网络圈子里的高手加入。安全厂商里真正懂网络的专家不是很多。”

网络技术功底深厚的张龙成为了奇安信交付运营的负责人，一干就是八年，从零开始，带起了一支千人团队。“我们的这支队伍在中国大型网络安全工程的交付运营队伍里是排在第一的。我们的大型网络安全工程交付运营不管从数量、质量还是营收额上，都远超同行。”

## 迎难而上 全面工程化

2021 年 4 月，张龙接到公司新的安排，接手区域发展中心，建设城市安全运营中心，发力安全托管业务。最初，这让张龙有些犯难。

安全托管服务，顾名思义即将网络安全运营等技术类工作委托给第三方代为管理，以服务化的形式帮助用户发现和解决各类安全问题。这项服务在国外已经非常成熟，在国内，随着数字城市建设的推进，同步规划城市数字化建设和信息安全建设，打造为数字城市保驾护航的安全底座，需要政府、社会和企业通力合作，安全托管服务也得以初步发展。除了国际上常见的 MSS 远程托管模式，在国内有一个特有的模式，就是通过产城合作的方法，建设城市网络安全运营中心。奇安信多年的发展，已经在很多城市初步试水合资公司的模式，开始了城市网络安全运营工作的推广。这些合资公司在不同的省份，工作模式千差万别，缺乏统一的经营和管理，业务规划上也千差万别；公司希望全国一盘棋，把这个创新的模式真正做起来。

“公司决定要换一个既懂经营又懂技术的人，就找我谈话。我当时有些犹豫，因为我以前没干过，觉得挑战挺大的，干交付虽然也有压力，但坦诚地说，工作难度没那么大。但是我后来想了想，这块业务确实非常重要，应该由一个对客户了解的技术负责人去接，而我以前在售前、产品经理、交付都干过，既然找到我，我就接吧。”

虽然做决定的时候有些犹豫，但一旦正式接手，张龙工程师的专注劲儿就完全上来了。“我们就是把原有的关于城市安全运营中心的想法，真正细化落地，把中心的建设进行了工程化。这是我们这帮人的特点。”

工程化也就是流程化、标准化。到一地后，张龙带团队先和当地网信办、大数据局等城市网络安全业务单元进行洽谈。初步达成一致后，几方一起详细列明工作内容清单，然后就针对性地洽谈团队。

“团队的规模根据工作内容而定，可以是我们自己完全承接，也可以是和国资方成立合资公司。什么样的情况需要成立合资公司？通常来说，如果要深度进行城市电子政务外网的运营，就需要成立合资公司，解决团队的身份问题。因为网络安全有一个特点，权限太大了，我们等于拿着别人的家门钥匙。我们对技术团队的人员组成的数量和质量都有相应的要求。合资公司谈成了、启动了之后，再去逐步地把团队按照计划一点点码起来。”

在张龙的工程化管理下，洽谈和成立城市安全运营中心有了一套规范流程，流程中的每一项工作都有了相对标准的要求。

## 想方设法 当好娘家人

无论是内部还是外部，一个城市安全运营中心的搭

建和运营过程中会遇见各种难题。因此，除了制定工程化的流程，张龙和团队还得沉下心解题。

张龙刚接手的时候，就发现一个难题。“在具体业务推进的时候，公司内部前、后台有不同的关注点。前台往往想加快推进的节奏。但是后台的法务、财务等风控部门则有疑虑，这是投资行为，必须审慎。我们这个团队成立以后，首先就是解决大家对话的问题。我们把前台的话翻译成业务逻辑，讲给后台，不解决公司的业务营收问题，连管控的机会都没有；再把后台的管控逻辑告诉前台，后台专家是替你们着想，成立一家公司背后有巨大的商业风险，做好了没有问题，做砸了，公司倒闭，导致国有资产流失，你们将承担后果。”

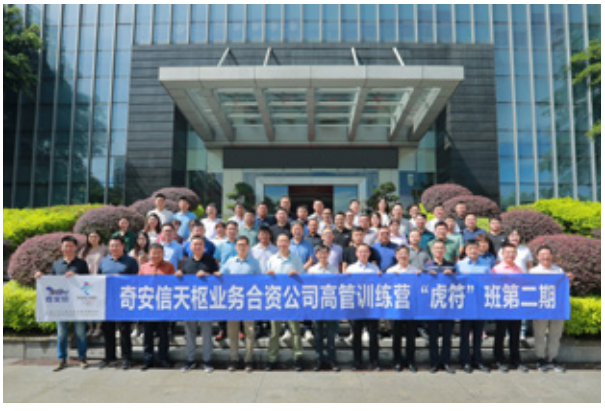
相比较理顺内部关系，张龙和团队遇到的第二个难题，显然更加棘手。“难题来自业务层面，也就是国资方的管控要求。举个例子，合资公司一旦出现一个季度的亏损，国资方就会很难接受，可能就要召开董事会问责。但是网络安全产业通常就是上半年没生意，下半年来生意，所以上半年就是亏损的。公司要用头一年的利润撑过第二年上半年，第二年下半年才赚钱，年底看是盈利的。网安行业刚启动的团队肯定会亏损，因为要招兵买马，要把这个团队建成当地最强，市场化这条腿才能强壮。但是坦诚说，一些国资方的领导就守着国资的规矩。为了解决这个问题，我们真是掰开了、揉碎了做国资方领导的工作。”

如果不能直接做通国资方领导的工作，张龙就曲线救国。有一次，某地的国资方一直不批合资公司的招聘预算。后来该地的市长到奇安信北京总部参观交流。交流现场，张龙抓住机会，直接建言：“领导，咱们成立了合资公司，就是一家人了，您得帮帮我们。我们现在有几个专家招聘不上来，说给的工资太高，但是网络安全圈子专家的薪水就是这个标准。我们承诺公司能赚到钱，所以是否能不拿国资那套薪酬体系卡着我们？”张龙的直言得到了市长的支持，市长现场跟合资公司的国资方领导表态：“经营的事情，你就听张总的，他亏本了，我找他，不找你。”

国资有自己的体系，企业有自己的制度，网安行业


城市网络安全运营中心高管培训（一期）

还有自己的特点，所以合作中问题和难点会持续性地出现，要持续性地解决。对此，张龙并不畏惧。“我们这个团队就是要当好娘家人，去跟国资方持续辩论。因为不这样，那些合资公司里我们派过去的总经理可能就没法干活。我们每年还要办两期总经理培训，具体讲授工作该怎么开展。这些总经理相当于所在城市的 CSO，他们的思维模式非常重要，不能是简单地买产品，而是要真正地解决问题。我相信这些点其他的安全公司可能都没碰到，因为他们没有像我们做得这么深，这么务实。”




城市网络安全运营中心高管培训（二期）

## 量身打造 三种运营模式

精准的定位、务实的作风，让奇安信的安全托管业务有声有色地发展了起来。根据业务的体量，张龙为数字城市相关行业及单位量身打造了三种不同的运营模式。即围绕政府数字化改革重点领域和方向开展的城市安全运营模式；围绕政府、大型央企及重点行业数字化转型发展战略开展的综合安全运营模式；围绕城市新兴战略型企业常态化网络安全需求开展的托管安全运营模式。


全国运营中心一盘棋

“业务体量不同，采取的运营模式就不同。特别大的城市，如广州和北京，我们就切了这个城市里的一个行业，即地方国资。因为这两个城市的国资太发达了，广州的国资有 5000 多家法人实体，北京有 7000 多家，这些公司的网络安全做得比较薄弱。我们先签约一家，做成标杆，然后再跟地方国资委谈，做市场化拓展。目前，我们与北京国资委下面的铜牛信息、广州国资委下面的广电运通，都成立了合资公司，运作情况都很好。”

截至目前，奇安信已在各地建立了 16 家合资公司开展安全托管业务，并成为了奇安信整体经营的重要一环。合资公司是为了城市的网络安全成立的，工作过程中，逐步取得了当地政府和企业的高度信任。所有建立了合资公司的地方，我们的市场占有率比我们的平均值高很多。除此之外，我们还多了外围的生态。我们现在已经有 200 多名率属于合资公司的工程师，在网络实战攻防演习等特定时期，这支团队可以调动。以前我们的技术团队基本上只能到省会一级，现在哪有合资公司，哪就有我们的一支 10~50 人的技术队伍。在三四线城市，你有一支这样的技术团队，你的销售腰杆得硬成什么样？他完全可以跟领导说，这活别人都接不了，就我能接！”

## 放眼未来 让城市更安全

实践已经证明奇安信目前的城市安全运营中心建设思路对、步子稳。而接下来，张龙已有了新的计划。

“我要把全国各地的城市安全运营中心打通，包括数据和运营规范。这实际也是进一步工程化的过程，完成以后，就能在全国下一盘大棋。同时，我也在思考一种新的运营模式，就是和运营商合作。中国电信、中国移动有大量的政企客户，这些客户以前托管的都是带宽，我们能不能把安全这一块加进去？最后，我还要把各地合作中的产教合作这块短板补上，形成真正的实战化的教学体系，培养出来的毕业生，就能直接在地方设立的安全运营中心实习，优秀的可以留用。这就解决了当地的网安人才问题。这条路径打通之后，整个的产城合作路径就打通了。”

从干交付轻车熟路，到干城市安全运营中心直面挑战，张龙骨子里还是那个严谨、专注、务实的工程师，但也有了新的思考、新的收获。“以前做交付，这个的工种特点相对被动，虽然我们也是积极主动去做一些事情，但它就是一个个项目、一个个客户，我们把它支撑好、服务好就行，思维模式比较简单。现在做城市网络安全运营中心，是要把一个生意从头至尾完全盘活的一个过程，其中要考虑的问题就复杂多了，所以做成了，自己的成就感不言而喻。城市安全运营中心对我来说，仍然充满挑战，但既然选了这项事业，我就要尽心尽力把它做好。城市让生活更美好，我们让城市更安全。”

未来，奇安信悉心打造的城市安全运营中心将在更多城市落地生根，张龙将带领团队把奇安信 MSS 带上一个更高的台阶。安

◀ 国家网络安全产业园区（长沙）城市网络安全运营中心



▲ 奇安信安全运营调度中心

▶ 宜昌城市级网络安全运营中心


▲宿州智慧城市运营中心


◀宜昌城市级网络安全运营中心

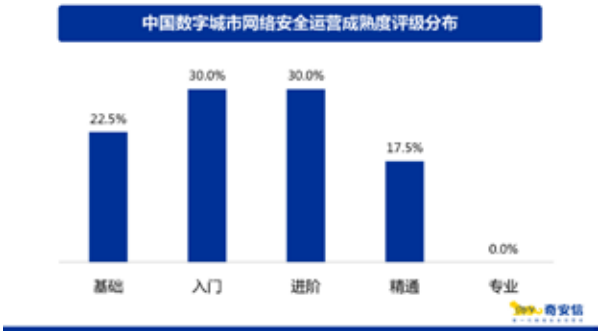
◀北京铜牛奇安科技有限公司安全运营中心

# 奇安信发布中国首个数字城市网络安全运营成熟度模型

作者 公关部 王梦琪

7 月 21 日，奇安信区域发展中心、奇安信行业安全研究中心、奇安星城网络安全运营服务（长沙）有限公司联合相关机构，正式发布了《2022 中国数字城市网络安全运营现状分析报告》（简称《报告》）。

《报告》首次提出了中国数字城市网络安全运营成熟度模型，通过“战略和规划”“流程和监管”“技术和服务”“人才和经验”“合规建设”五个维度，对国内 40 座不同类型的城市（国家中心城市 7 座、中心城市 16 座、非中心城市 17 座）安全运营水平进行评估。结果显示，半数以上城市的网络安全运营成熟度均处于基础和入门阶段，水平相对较低，暂无城市能够达到最高等级“专业”级。




## 危机四伏的数字城市安全环境

城市数字化进程的高速发展，使得网络安全问题的

影响不断凸显。以勒索、挖矿、APT 等为代表的新型网络攻击活动的持续活跃，引发了全球每年数以千计的重大网络安全事件，工厂停工、城市停摆的新闻屡见不鲜。数字化的城市正面临着网络安全的重重危机。

2021 年 2 月，美国佛罗里达州水处理系统遭黑客攻击，攻击者试图将氢氧化钠的浓度从百万分之 100 更改为百万分之 11100。操作员及时发现了异常才阻止了“灾难”。

2021 年 5 月，美国最大的燃油管道商 ColonialPipeline 遭到勒索软件攻击，导致该公司暂停了所有的管道作业网络，并关闭了一条主要的燃料传输管道。美国交通部被迫采取紧急措施，放宽了 17 个州的公路运油限制，以免各地燃油短缺。

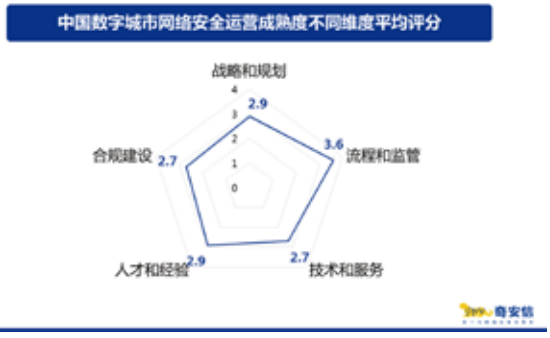
2021 年 7 月，伊朗铁路系统遭遇网络攻击，攻击者在全国各地车站的显示屏上大肆发布关于火车延误或取消的虚假信息。

2022 年年初发生的俄乌冲突，进一步加剧了人们对数字城市的安全担忧。在物理战场之外，包括俄乌在内的多方势力，在网络空间这个看不见硝烟的第二战场上激烈较量，对城市的安全运营造成了前所未有的冲击。

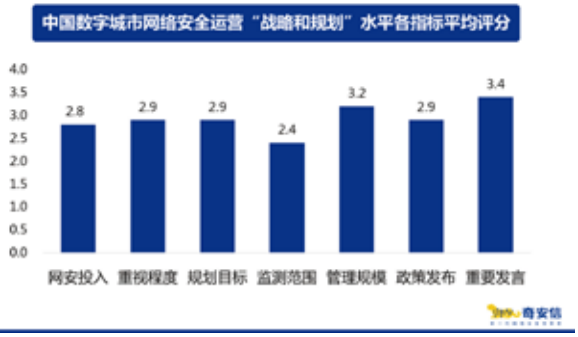
奇安信集团副总裁张龙表示，目前国际环境日趋复杂，全球产业链供应链遭受冲击，网络空间安全面临的形势持续复杂多变。此外，随着数字化、网络化进程加快，城市资产暴露面不断扩大，安全漏洞、数据泄露、网络诈骗等风险持续增加。在此背景下，数字城市建设、运营和治理等方面的工作重心也发生了重大的变化，数字城市网络安全的构建需要满足城市自身数字化转型对网络安全保障的要求。


## 数字城市网络安全运营存在明显短板

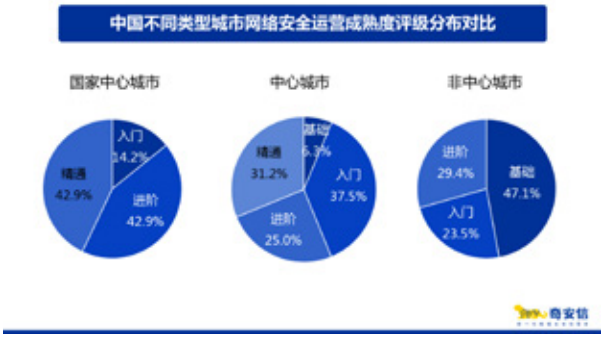
从评价数字城市网络安全运营成熟度的五个维度来看，“流程和监管”的整体水平相对最高，40 座城市的平均评分达到 3.6 分（满分 5 分），对应“进阶”级别。而“战略和规划”“技术和服务”“人才和经验”“合规建设”这几个方面，全国各城市的总平均分仅达到 2.7~2.9 分。




值得关注的是，在其他各个维度中，至少有 5% 以上的城市可以达到“专业”等级，但在“战略和规划”方面，目前尚没有任何城市可以达到最高等级的“专业”水平，存在明显的短板。




具体而言，在“战略和规划”的七项指标中，仅有两项的全国平均分在 3 分以上。这也意味着 dous，国内城市在“战略和规划”方面，整体处于较低水平。平均分最高的是“重要发言”。从中可以看出，大多数城市的领导都非常重视网络安全工作，并在近两年做出过重要的发言或表态。




“监测范围”是得分最低的一项，全国平均分仅为 2.4 分。这一数字表明，国内绝大多数的城市只能达到对部分关键信息基础设施的安全监测与运营，而没有实现行业级的网络安全监测与运营能力，更不用说城市整体的网络安全监测与运营能力。

相较之下，在“流程和监管”方面，有半数的城市可以达到“精通”和“专业”水平，并且相关六项指标全国平均水平均在 3 分以上。其中，“主管部门”和“规范文档”的这两项平均分最高，为 4.1 分。这就说明，绝大多数城市的网络安全工作都有明确的主管部门，能够建立一批“城市级重要网络安全信息规范文档”，使得本市的网络安全工作能够有据可依、有序开展。

显然，这是近年来国内各地持续不断地加强网络安全监管力度，所取得的重要成果。

## 不充分、不均衡的数字城市安全运营发展

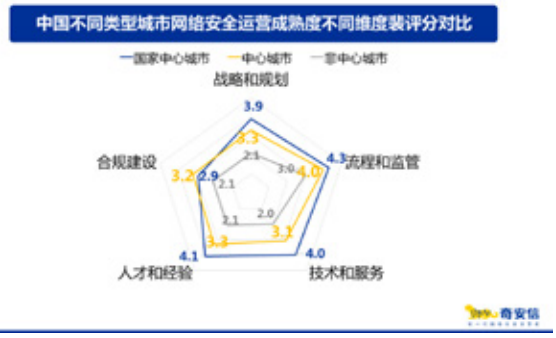
不过，不同类型、不同经济规模、不同数字化程度的城市，对于网络安全运营成熟度的要求也有所不同。

调查结果显示，所有的国家中心城市都已经完全摆脱了最低评级“基础”级，而达到“精通”和“进阶”这两个级别的城市都超过了四成，但仍有个别城市仅达到“入门”级别。

相比于国家中心城市，中心城市的评级分布比较平均，除了 5.3% 的城市为“基础”级，达到“入门”“进阶”和“精通”级别的城市分别占比为 37.5%、25.0% 和 31.2%。仅达到“基础”和“入门”级别的城市占比超过四成。这说明，中心城市的网络安全运营成熟度水平与国家中心城市相比要落后很多。

不过，非中心城市的成熟度水平较国家中心城市、中心城市都要低得多，47.1% 的城市仅能达到最低评级“基础”级别。仅有 29.4% 的城市能够达到中等水平的“进阶”级别，没有任何被调研的城市能够达到“精通”及以上的级别。

并且，非中心城市在各个方面都显著落后于中心城市和国家中心城市，只有“流程和监管”这一个维度的全国平均分能够达到 3.0 分，其他各个维度的全国平均分均为 2.0~2.1。




考虑到实际情况，非中心城市的比例要远远多于此次受调研的 40 座城市中的占比情况，因此我国的数字城市网络安全运营工作任重而道远。

为此，奇安信已于 2021 年 5 月正式成立区域发展中心，以建设城市运营中心、企业综合运营中心、提供远程托管运营服务等业务模式，为地方政府、大型企业、中小企业建设体系化、实战化、常态化的网络安全运营体系。

据张龙介绍，区域发展中心成立一年多来，奇安信与当地的网信办、大数据管理局深度合作，成立国资背景为主的城市安全运营中心，数据本地化、服务本地化，奇安信全面提供技术支撑与信息服务。截至目前，奇安信已经建设了长沙、北京、广州、德阳、安庆等十几个城市安全运营中心。安

## 大事记

### 奇安信与数字广东签署战略合作协议 携手推动广东数字政府建设

8 月 16 日，奇安信集团董事长齐向东与数字广东公司党委书记、董事长李恒白签署战略合作协议，奇安信与数字广东正式达成战略合作。

根据协议，奇安信将从信息安全咨询规划、解决方案设计出发，积极协助数字广东进行安全体系建设和运营，以及完善内部信息安全管理制度。而数字广东公司将继续夯实网络安全底座，有效提升数字政府系统的安全运营水平，保障广东“数字政府 2.0”建设和构建数字政府“12345+N”工作业务体系顺利推进。


### 奇安信与十家央企举办北京冬奥网络安全“零事故”分享会

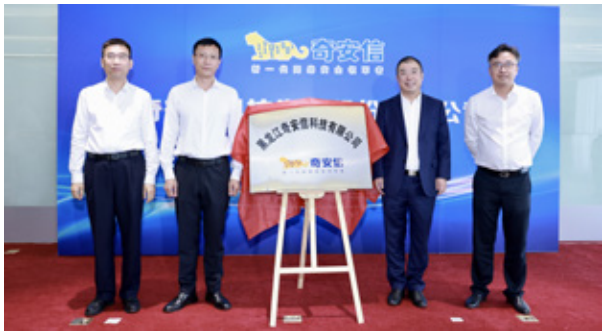
8 月 16 日，中国电子—奇安信与十家央企在深圳举办了北京冬奥网络安全“零事故”经验线下分享会，来自中国南方航空、华侨城集团、招商局集团、中广核、南光集团、中国旅游集团、紫荆文化集团，以及中国电子及其旗下的中国系统、中国软件、麒麟、飞腾共 10 家企业的领导与负责人出席会议并交流，与会嘉宾就冬奥“零事故”经验、央企数字化建设、信创构建与发展等方面进行了深入的交流与讨论。


### 黑龙江省政府与奇安信达成战略合作 奇安信黑龙江子公司正式揭牌

8 月 11 日，在 2022 世界 5G 大会黑龙江招商引资项目签约仪式上，黑龙江省政府与奇安信集团正式签署战略合作协议。围绕北方区总部暨区域安全运营中心项目，黑龙江省政府与奇安信在网络安全领域达成全方面合作，助力“数字黑龙江”安全稳步发展。

此次合作，黑龙江省政府与奇安信将在城市网络空间安全治理、数字城市安全体系建设、自主可控、工业互联网安全、大数据安全、人才培养、网络信息安全产业发展等领域开展深入合作。

作为战略合作的重要内容之一，黑龙江奇安信科技有限公司于签约当天正式揭牌。



## 齐向东出席 2022 世界 5G 大会：以“零事故”为目标护航 5G 融入千行百业

8 月 10 日，在 2022 世界 5G 大会主论坛上，奇安信集团董事长齐向东表示，5G 应用发展加速了各行各业的数字化转型，同时也面临着更加复杂的网络安全挑战。当前，我国 5G 应用正处于规模化快速发展的关键阶段，要以“零事故”为目标，护航 5G 融入千行百业，筑牢安全底板。

齐向东表示，冬奥网络安全保障的结果已证明，网络安全“零事故”是可以实现的目标，奇安信也以“零事故”为目标，梳理 5G 应用的共性网络安全需求，融合形成了统一的安全架构，助力 5G 应用快速发展，护航 5G 融入千行百业。而实现“零事故”目标，需满足“联合作战、精准防护、深度运营”三大要求。


## 齐向东出席全球数字经济大会：产业数字化转型需做好“三防”

7 月 29 日，在 2022 全球数字经济大会开幕式暨主论坛上，奇安信集团董事长齐向东表示，健全我国数据安全保护体系，需要从“守法、投钱、培养人”三个方面不断完善；企业则应该做到“防违法、防盗窃、防勒索”。

在全球数字经济大会数字经济产业园区发展论坛，齐向东表示，数字城市的首要挑战是网络安全，而当前，我国城市安全运营存在明显短板，半数以上城市处在基础和入门阶段。要增强数字城市的抗风险能力，需要以“零事故”为目标，打造数字城市“零事故”的中国方案，建设数字城市网络安全体系。


## 2022 安全创客汇总决赛落幕 为辰信安荣膺全国总冠军

7 月 27 日，由奇安信集团、北京网络安全大会、全国网络信息安全创业投资服务联盟（筹）、奇安投资、中电智慧基金联合主办的 2022 安全创客汇总决赛圆满落幕。

广东为辰信息科技有限公司从十强企业脱颖而出，夺得冠军，并现场与奇安投资签订 2000 万元的投资意向书。安易科技（北京）有限公司、北京方研矩行科技

有限公司（简称“青莲云”）、杭州亿格云科技有限公司分别获最具创新力奖、最具市场潜力奖和最佳团队奖。


## 奇安信发布《2022 中国软件供应链安全分析报告》

7 月 26 日，奇安信集团对外发布了《2022 中国软件供应链安全分析报告》，对过去一年多来国内软件供应链各个环节的安全形势，进行了深入细致的分析。

《报告》显示，与前一年度相比，企业自主研发源代码安全缺陷情况有明显改善，千行代码缺陷密度和十类典型安全缺陷的总体检出率均有明显下降，这应该得益于软件源代码安全缺陷分析工具的持续应用，以及程序员编写代码时安全意识的提高。但开源软件安全风险仍然居高不下，开源软件的安全风险管控是当前软件供应链安全保障需要解决的核心焦点问题。


## 齐向东出席数字中国建设峰会：以“零事故”为目标保护云上数据

7 月 23 日，在第五届数字中国建设峰会上，奇安信集团董事长齐向东在主题演讲中表示，要以“零事故”为目标保护云上数据。通过建立“三方制衡”机制、联合作战、精准防护、深度运营、应急响应五大措施，做到云业务不中断、数据不出事、合规不踩线。


## 荣誉墙

## 星舆实验室获评 AutoCS 2022 年度杰出智能网联汽车安全研究实验室

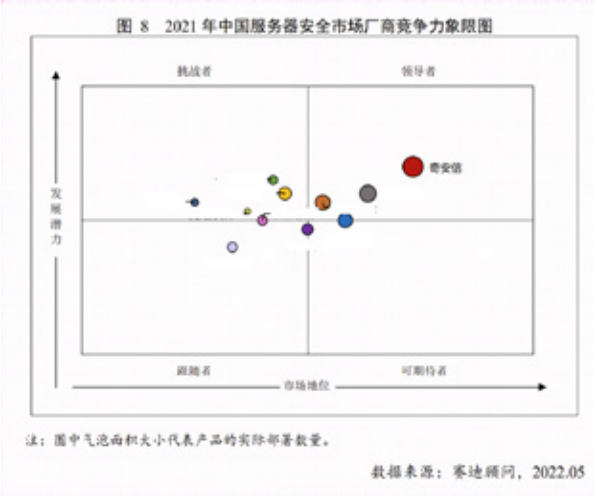
8 月 18 日至 19 日，AutoCS 2022（2022 智能汽车信息安全大会）在上海举办。会上，奇安信星舆实验室因对车联网安全行业的突出贡献与杰出实力，经过会议专家层层筛选后，获评 AutoCS 2022 年度杰出智能网联汽车安全研究实验室。

会上，星舆实验室安全研究员范鹏还发表了《车内通信框架安全分析与防御》的主题演讲，向大家分享了在面向服务的漏洞挖掘中对车内通信安全的心得体会，

介绍车内常用通信（IPC、RPC）框架，以及存在的安全威胁、分析方法及防御措施。


## 赛迪顾问发布中国服务器安全报告 奇安信稳居市场第一

近日，权威机构赛迪顾问发布《中国服务器安全市场研究报告（2022）》，详细分析了中国服务器安全市场的发展情况、发展趋势和竞争格局。《报告》指出，2022 年中国服务器安全市场规模将达到 79.7 亿元，其中，奇安信椒图云锁服务器安全系统的市场地位、发展潜力和部署总量均为中国第一。




赛迪顾问指出，随着越来越多的信息通过云端传递，已经有越来越多的企业采用云服务器，云服务器的安全性也受到了众多用户的重视，中国云服务器安全市场将迎来快速增长。目前，中国服务器安全市场竞争较为激烈，从市场地位上来看，奇安信凭借多个较大型项目，以及与其他产品协同配合的整体解决方案等优势，在市场规模及部署量方面均处于领先地位，行业覆盖面广，市场认同度较高。

## 首次上榜！奇安信被评为 Gartner 智慧城市 CPS 代表供应商

近日，围绕“政府数字化转型和创新”这一主题，国际研究机构 Gartner 正式发布了《Hype Cycle for Smart City and Sustainability in China, 2022》报告，“将帮助地方政府和城市生态系统合作伙伴的首席信息官评估实现数字社会和可持续发展成果的新兴技术和解决方案。”其中，在智慧城市中的信息物理系统（CPS）安全领域，奇安信作为样本供应商首次被列入该报告。

作为网络安全龙头企业，奇安信一直在努力解决智慧城市的网络安全问题，通过坚持培育统一的安全运营能力、坚持打造无懈可击的安全运营闭环、坚持用实战演练提升安全运营效果的“三个坚持”，积极打造城市安全运营中心的中国模式。接下来将以“零事故”为目标，深入推进城市安全运营中心建设。

据介绍，奇安信于 2021 年 5 月正式成立区域发展中心，以建设城市运营中心、企业综合运营中心、提供远程托管运营服务等业务模式，为地方政府、大型企业、中小企业建设体系化、实战化、常态化的网络安全运营体系。奇安信从智慧城市的实际安全需求出发，制定了城市安全运营中心的理论框架、技术架构和实施策略，并先后在国内二十多个城市落地实施。截至目前，奇安信已经建设了长沙、北京、广州、德阳、安庆等十几个城市安全运营中心。

## 奇安盘古隐私卫士荣获 2022 年数据安全典型实践案例

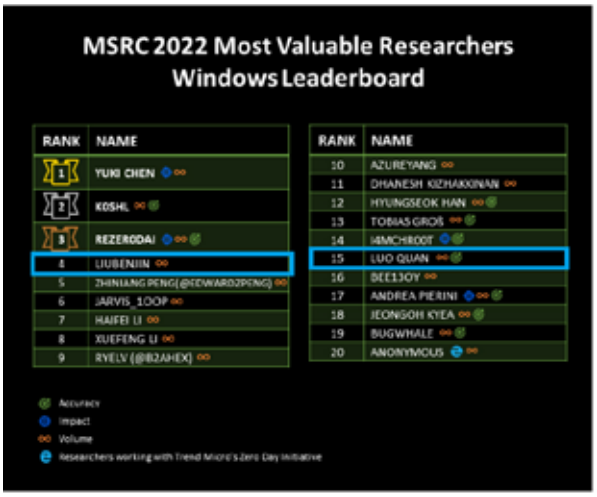
近日，在 2022 数字安全与法治高峰论坛中，奇安盘古凭借在移动数据安全领域的多年实践经验再获认可，奇安盘古隐私卫士软件（简称“隐私卫士”）荣获中国网络空间安全协会颁发的 2022 年“数据安全典型实践案例”。

推动数据开发利用和数据安全融合发展，尤其强调对个人信息和用户隐私的保护，奇安盘古隐私卫士软件，通过技术手段辅助发现隐私安全风险，以解决由此带来的数据泄漏、资产损失、监管处罚等风险，为目前面临的数据安全保护场景、数据安全合规面临的几大关键问题，提供了防护。


## 奇安信代码安全实验室三人入选“MSRC 2022 全球 Top 100 最具价值研究者”榜单

8 月 9 日，微软安全响应中心 (MSRC) 发布 2022 年度全球 Top 100 最具价值研究者榜单，奇安信代码安全实验室的三名研究员，凭借高超的安全漏洞研究能力入选该榜单，分别位列第 7 名、第 15 名和第 47 名。

此外，微软还发布了四个特定技术领域的荣誉榜单，分别是 Windows 操作系统榜单、Azure 云榜单、Office 榜单、Dynamics 榜单。奇安信代码安全实验室的两名研究员，入选“MSRC 2022 最具价值研究者——Windows 操作系统榜单”，分别位列第 4 名和第 15 名；一名研究员入选“MSRC 2022 最具价值研究者——Azure 云榜单”，位列第 4 名。




## 国内唯一大型供应商！奇安信入围权威机构托管安全服务报告

近日，国际权威咨询机构 Forrester 发布《The Managed Security Services Landscape In Asia Pacific, Q3 2022》报告，在亚太地区的 25 家供应商中，基于 MSS 服务和市场规模，奇安信作为唯一一家大型供应商被选入该报告。该报告从市场定义、商业价值和市场动态等方面分析亚太地区托管安全服务（MSS）市场现状及发展，帮助政企组织相关人员获得更多 MSS 方面的安全专业知识。

值得一提的是，相比于去年，奇安信 MSS 已经从中型供应商梯队进阶为大型供应商梯队，并成为大型供应商梯队中唯一入选的国内安全厂商。在短短一年内，奇安信 MSS 凭借发展规模和增长速度跻身亚太地区头部供应商梯队，其综合实力获得了国际认可。

## 首家、唯一、全品类！奇安信数据安全通过全系列认证

7 月 28 日，由中国信息通信研究院（以下简称“中


国信通院”）安全研究所主办，数据安全共同体计划和大数据应用与安全创新实验室承办的“数据安全峰会 2022”在北京召开。本次峰会公布了最新一批数据安全产品能力验证名单，奇安信旗下多款数据安全产品，全部通过了中国信通院在开展的七大品类的测评认证，成为首家获得全套数据安全产品测评资质证书的网络安全企业。

现场，主办方为通过“数据安全产品能力验证计划”的企业颁发了“数据安全产品能力专项检验证书”。奇安信围绕 7 大类别，分别提供了数据库审计、API 安全卫士、数据安全态势感知平台、敏感数据发现和分类分级系统、数据脱敏系统、数据水印系统等对应的数据安全产品，并一次性全部通过测评认证，成为迄今为止数量最多、品类最全、覆盖最广的网络安全企业。

## 奇安信获 2022 云生态大会“最具价值云应用合作伙伴”奖

7 月 24 日，在第五届数字中国建设峰会 · 云生态大会上，奇安信荣获天翼云 2022 年度“最具价值云应用合作伙伴”奖。

奇安信自 2021 年开始与天翼云合作，已在全国累计开展 30 多个安全资源池建设，从技术方案、产品交付等方面实现了全流程协同。其中，由奇安信助力中国电信打造的天翼攻防网络实战平台，获评“天翼网信安全产业联盟优秀安全实践案例”。

2022 年 1 月，中国电信天翼云公布 2021 年云资源池安全产品集中采购候选人名单，奇安信集团旗下的网神公司以综合排名第一的成绩，成为该项目第一中标候选人，充分体现了天翼云对奇安信云安全实力的认可。


## 奇安信 NGSOC 荣获 2022 数字中国“十佳解决方案”


7 月 24 日下午，第五届数字中国建设峰会最佳成果颁奖仪式在海峡国际会展中心举办。奇安信态势感知与安全运营平台（简称 NGSOC）凭借在 2022 北京冬奥网络安全“零事故”保障中的突出表现，从数百家参选方案中脱颖而出，荣获 2022 数字中国“十佳解决方案”，并成为唯一获得该项荣誉的网络安全厂商。

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

# “零事故”

## 奇安信圆满完成冬奥会网络安全保障任务

# 奇安信蝉联“中国网安产业竞争力50强”第一名


6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信蝉联第一名。


**“2022年中国网安产业竞争力50强”榜单**

| TOP15 | 公司名称 |
|---|---|
| 1 | **奇安信科技集团股份有限公司** |
| 2 | 深信服科技股份有限公司 |
| 3 | 启明星辰信息技术集团股份有限公司 |
| 4 | 天融信科技集团股份有限公司 |
| 5 | 华为技术有限公司 |
| 6 | 绿盟科技集团股份有限公司 |
| 7 | 腾讯云计算（北京）有限责任公司 |
| 8 | 阿里云计算有限公司 |
| 9 | 新华三技术有限公司 |
| 10 | 杭州安恒信息技术股份有限公司 |
| 11 | 360政企安全集团 |
| 12 | 亚信安全科技股份有限公司 |
| 13 | 成都卫士通信息产业股份有限公司 |
| 14 | 杭州迪普科技股份有限公司 |
| 15 | 山石网科通信技术股份有限公司 |