SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

我们是网络安全中国代表队

经营安全 安全经营

——2021 北京网络安全大会特刊

第 9 期

2021 年 9 月

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器

纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

政企实施网络安全的“三部曲”

2021 北京网络安全大会 (简称 BCS 2021) 以云峰会形式盛大启幕。十余位两院院士，200 多位全球嘉宾齐聚云端，如往年一样精彩纷呈。

BCS 2021 以“经营安全，安全经营”为主题，这读起来稍显绕口的八个字，却包含着思辨的逻辑关系和 DT 时代的价值观。经营安全、安全经营不是无源之水，无本之末。

回顾前两届北京网络安全大会的主题：2019 年主题——内生安全，其意是将安全能力内置到信息化的环境中，从某种角度上看，它是 DT 时代的安全理念。2020 年主题——内生安全框架，其意是通过系统工作的方法建成内生安全体系，这是将内生安全理念落地的方法。2021 年的主题——安全经营，经营安全，其意在于只有用心的去经营安全体系，才能保障经营活动的安全运转。

从 2019 年到 2021 年，北京网络安全大会三年的主题，如奇安信董事长齐向东在主题演讲中所指说，共同组成了政企机构实施网络安全的“三部曲”：理念、方法、动态掌控。

2021 年网络安全迎来新拐点。今年以来，随着“十四五”的到来，数字化开始贯穿经济社会发展的全领域、各层级，成为国家治理、经济发展和社会运行的核心驱动力。今年以来，《数据安全法》《关基保护条例》《个人信息保护法》《网络安全审查办法》修订版等法律法规、政策制度和监管手段密集出台。网络安全与此同时也成为中国数字化建设的工作重点之一，网络安全迎来了发展新拐点。

面对新的安全形势和合规需求，网络安全需要拥抱新范畴、新管理、新模式和新范式，转向以能力为导向的、信息化跟网络安全深度融合的建设模式，方能化挑战为机遇。

面对 DT 时代网络安全的颠覆性变化，如何通过安全运营，经营好您的安全系统，从而形成良性循环，是接下来要靠规划和落实的要务。

总编辑

李建平

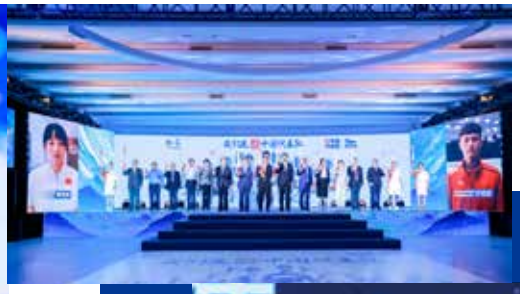
2021 年 9 月 1 日

CONTEN

目录

战略篇

领导致辞……04
经营安全才能安全经营 —— 齐向东 BCS 2021 演讲全文……10
DT 时代责任无界经营安全才能安全经营 ……18
本 · 以色列：揭秘以色列网络安全产业生态的发展之路 ……22
俄罗斯前副总理：两条规则保障网络安全……23
约翰 · 戴维斯：全球勒索攻击近乎“失控”抗衡需国际协同合作 ……24
郑永年谈网络世界“两极化”与安全发展……25
中外专家汇聚 BCS 共商数字世界竞合之路 ……26



产业篇

吴云坤：网络安全的新范畴、新管理、新模式和新范式……30
BCS 2021 产业峰会：网络安全产业迎来新拐点 ……36
构建网络空间法治基石，营造良好数字法治生态……40
2500 亿市场中国网络安全企业的机与责 ……43
探真科技荣膺总冠军新场景安全受热捧……45
护航数字经济发展，开拓产融安全机遇……47
内生安全引领金融新基建……49
数字城市安全论坛：建设防护体系，保障健康稳定运行……52

TS

技术篇

谭晓生：中国网络安全技术趋势分析…… 54
BCS 2021 技术峰会：攻与防的角力 经营安全推动网络安全技术变革 60
BCS 2021 聚焦“安全经营” 齐向东首提实战化态势感知 …… 64
数据安全与治理论坛成功举办数字经济发展应注重安全治理能力…… 66
隐私计算：可信应用实践与挑战…… 68
聚焦行业数字化建设 BCS 2021 工业互联网安全论坛在京召开 …… 70
InForSec 网络空间安全国际学术成果分享论坛成功举办 …… 72

成果篇

经营安全推动网络安全产品技术创新近 20 款网络安全产品重磅亮相 …74

第 9 期
《网安 26 号院》编辑部
主办 奇安信集团

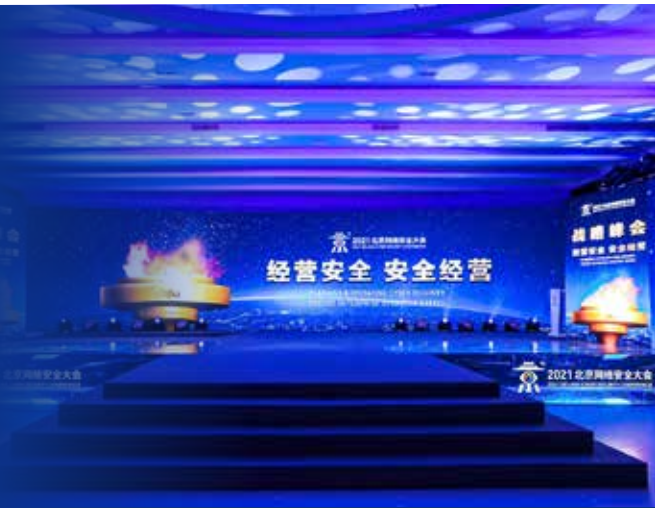
总编辑：李建平
副总编：裴智勇
战略篇：张文辉 包世玉
产业篇：李建平 王 彪
技术篇：张雪丹 孙丽芳
成果篇：魏开元

奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载
索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

Email: 26hao@qianxin.com
地 址：北京市西城区西直门外南路 26 院 1 号
邮 编：100044
电 话：（010）13701388557
出版物准印证号：京内资准字 2021- L0058 号
印刷数量：45000 本
印刷单位：北京七彩虹印刷有限公司

2021 北京网络安全大会（BCS 2021）领导嘉宾云集，原工业和信息化部党组成员、副部长刘烈宏，北京市委常委、副市长殷勇，中国电子信息产业集团董事长芮晓武，十三届全国政协社会和法制委员会副主任、中国友谊促进会理事长陈智敏，央网信办网络安全协调局局长孙蔚敏，公安部网络安全保卫局一级巡视员、副局长郭启全，北京2022年冬奥会和冬残奥会组委会副秘书长徐志军，全国工商联副秘书长、会员部部长郭孟谦，北京市西城区委副书记、区长孙硕等出席并致辞。



刘烈宏 | 原工业和信息化部党组成员、副部长

刘烈宏表示，我国网络安全创新发展取得了一系列积极成效，产业呈现三大发展亮点。其一，网络安全产业规模快速增长。2020 年产业规模超过了 1700 亿元，较 2015 年翻了一倍，年均增速超过 15%，远高于 9% 的全球平均水平。其二，技术创新能力明显提升。5G 安全、工业互联网安全、数据安全等一批关键技术取得突破，企业实力不断增强，企业投融资并购活跃，相关上市企业已经有 20 余家，总市值超过 5000 亿元。其三，产业聚集发展加速。北京、湖南、长沙、国家网络安全产业园相继成立，聚焦重点安全的企业超过 300 家，产业集聚效益持续放大。

要做到网安生态融合发展，刘烈宏提出三点建议：一是要积极鼓励龙头企业带动中小企业，促进产业链上下协同发展，强化安全能力整体输出，打好网络安全“团体赛”；二是促进资本对网络安全的支持，助力优质企业快速成长；三是加强产教协同、强化高水平网络安全人才建设，鼓励通过竞赛演练多种形式选才育才，加快推动形成市场化的网络安全能力评价机制，培育公平竞争的市场环境。

殷　勇 | 北京市委常委、副市长

殷勇指出，北京市将从以下四方面推动网络安全产业高质量发展。

一是大力发展数字经济，打造科技战略力量。北京将充分发挥好自身科技创新优势，加强网络安全人才建设，支持企业开展核心基础技术攻关，提升网络安全供应能力，推进“长安链”等自主创新应用与网信基础设施深度融合。

二是持续支持产业聚集，建设高水平产业生态。国家网络安全产业园已初步形成“三园协同、多点联动、辐射全国”的网络安全产业发展格局。北京将进一步推动园区高水平建设，在政策、资金、服务等方面做好工作保障，推动园区产业适配和产业生态建设，形成产业集聚效应。

三是探索建立数据安全管理体系，推动数据要素有效配置。北京将探索完善数据要素配置领域的体制机制，推动国际大数据交易所、城市超级算力中心、数据中心的建设，通过数据采集、存储、处理、交易、出境等应用场景拉动、推动网络安全产业对数据流转全流程安全保护的支撑。

四是坚持优化营商环境，推动产业开放发展。其中包括紧抓“两区”建设契机，加大开放力度，加强体制机制创新，争取更多政策试点，强化网络安全领域生态合作、国际合作、场景合作。进一步优化营商环境，加强网络安全产业企业服务，针对企业发展中的痛点、难点，落实好服务包和服务管家机制，为企业切实分忧解难，提升企业获得感。

芮晓武 | 中国电子信息产业集团董事长

芮晓武强调，产业融合发展更要加快推动网络安全防护融入信息系统建设。他表示，中国电子坚持应用场景需求牵引。从系统设计、运营管理、审查监管等各方面统筹网络安全防护和信息系统建设，强化管云、管数，增强面向安全运营的态势感知能力，加强数据全生命周期安全防护，持续输出安全能力，整体构建信息系统网络安全防护体系，确保信息系统运营安全。

芮晓武认为，应加快推动生态体系建设融入产业发展进程。中国电子着力协同创新和开放创新，注重生态体系建设。在网络安全技术应用等方面加强产学研用交流与联合创新，广泛凝聚创新合力，不断扩大创新发展“朋友圈”。在国际合作上，强化面向全球的业务布局和资源配置，全面提升国际化经营能力。他表示“期待继续与国内外生态合作伙伴在数字化转型、工业互联网、数据治理、云建设服务等重点领域关键应用和重大工程上共同推动实施一批具有前瞻性、引领性的网络安全合作项目，与产业界一道实现共赢发展。”

陈智敏 | 十三届全国政协社会和法制委员会副主任、中国友谊促进会理事长

陈智敏在演讲中表示，数据安全是网络安全的核心，党的十九届四中全会将数据明确为生产要素之一，参与分配，五中全会提出，要发展数字经济，推进数字产业化和产业数字化；建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范；保障国家数据安全，加强个人信息保护；积极参与数字领域国际规则和标准制定。《中华人民共和国数据安全法》即将实施。

陈智敏认为，要切实保护好数据安全还需要从理论上、法律上进一步解决数据权属问题。数据是新的生产要素、生产资料，是基础性资源和战略资源。这个问题不仅关系到数据安全，还关系到国家政治安全、社会公共安全、经济安全、文化安全、企业安全、公民个人隐私和财产安全、数字经济健康有序发展、人类社会的公平正义乃至前途命运。同时要贯彻落实好新发展阶段、新发展理念、新发展格局，坚持以人民为中心，实现共同富裕，实现高质量发展，处理好安全与发展的关系，这是一个回避不了、绕不过去，并且，必须解决的时代性、国际性、创新性问题。

孙蔚敏 | 中央网信办网络安全协调局局长

一是坚持网络安全为人民，网络安全靠人民。总书记指出江山就是人民，人民就是江山。人民对美好生活的向往就是党的奋斗目标，要把实现好、维护好、发展好广大人民群众在网络空间的合法权益，作为网络安全工作的出发点和落脚点，以办好 2021 年国家网络安全宣传为抓手，增强全民网络安全意识和防护技能，同时充分发挥人民群众在维护网络安全的重要作用，让人民群众成为网络安全的参与者、建设者、受益者，国家、企业、个人共同维护网络安全。

二是树立整体动态的安全防护理念，随着云计算、大数据、人工智能等新技术的应用普及，过去分散独立的信息系统，变的高度关联，相互依赖，系统边界日益模糊，同时网络安全的威胁样式和攻击手段也在不断变化，那种依靠安装几个安全设备和安全软件就想永保的想法，已跟不上时代，需要树立整体动态的防护理念，坚持系统观念，底线思维，积极防御，综合应对不断变化的安全风险。

三是加强关键基础设施保护和数据安全管理。关键信息基础设施是经济社会运行的神经中枢，是国家安全工作的重中之重，要做好关键基础设施安全保护条例宣贯解读和贯彻落实，完善信息基础设施安全保护制度，强化政府指导和监管，压实各方面责任，特别是压实关键基础设施运营者主体责任，全面增强态势感知、监测预警、风险评估、事件促治、灾难恢复等，实现关键技术可控的途径，把产业作为网络安全能力的重要内容和支持网络安全教育的动能。

郭启全 | 公安部网络安全保卫局副局长、一级巡视员

第一，今年国家网络安全相关的法律法规和政策标准密切出台。《数据安全法》《关键信息基础设施安全保护条例》《个人信息保护法》等政策相应出台。这些法律政策的密切出台，为开展网络安全工作、推动网络安全产业发展，提供了很好地支持。2021 年是关键信息基础设施安全保护元年，数据安全保护元年，个人信息保护元年，这三个元年和等级保护 2.0 制度配合起来，表明国家网络安全工作已经进入到 2.0 阶段。进入一个新时代，就要有新作为、新举措、新目标、新高度。

第二，一系列法律法规和制度该如何实施。比如，网络安全等级保护制度，关键信息基础安全保护制度，数据安全保护制度，个人信息保护制度，如何在中央的大的战略布局和相关政策法规标准的保障下，把这些制度有机地结合起来去实施，成为当下关注的重点。因此，需要在原来工作基础之上，多部门密切配合，多制度有机结合，全社会共同将制度有机衔接好，组织好，落实好。

第三，法律政策标准密集出台，特别是中央，已经出台了“十四五”网络安全和信息化战略规划，今后几年的工作重点是如何落实这些制度。网络安全工作要以问题导向，实战引领，体系化作战，在总书记和党中央的坚强领导下，各部门和社会各界要密切配合，构建网络安全综合防御体系，按照打防管控一体化要求，相关职能部门要把统筹协调工作做好，把监管工作做好，把违法犯罪打击工作做好。

徐志军 | 北京 2022 年冬奥会和冬残奥会组织委员副秘书长

徐志军表示，网络安全是冬奥筹办工作的重要内容。北京冬奥组委高度重视，制定实施了全面网络安全战略，不断优化系统设备、完善防护措施，确保冬奥场馆信息基础设施和各平台系统具备内生安全能力。

徐志军还表示，习近平总书记强调，“安全是重大体育赛事必须坚守的底线”，这为做好冬奥筹办工作提供了根本遵循。北京冬奥组委将与各方紧密合作，做好冬奥网络安全工作，确保赛事如期安全顺利举办，共同为世界奉献一届“简约、安全、精彩”的奥运盛会。

郭孟谦 | 全国工商联副秘书长、会员部部长

对于筑建网络安全防线，郭孟谦在会上分享了以下三点建议。

一是网络安全企业要与国家安全同步经营。据统计，2021 年上半年，我国共有 4500 多家公司开展网络安全业务，相比上一年增长了 23.1%。结合国家网络安全法、数据安全法、网络安全审查办法、个人信息保护法、网络安全产业高质量发展三年行动计划等法规政策来看，安全企业既要看到国家的政策保障，树立对网络安全业务发展的信心，也要看到风险警示，勇于挑起企业责任担当。

二是网络安全产业要为数字经济发展保驾护航。郭孟谦介绍，民营企业要有自己过硬的技术。在全球数字化转型趋势的指引下，5G、云计算、大数据、物联网、人工智能等新一代信息技术高速发展，如何才能应对日趋激烈的国际竞争？唯有充分掌握网络安全自主创新知识产权和核心技术，才能避免在关键时刻“卡脖子”的技术难题。

三是网络安全需要各方携手合作。在复杂的国际经济政治格局中，各个国家面临着两点相同的问题：一是都在迎接数字经济的发展浪潮，二是都要面对网络安全的威胁挑战。这种形势下，广大民营企业要善于通过网络安全与各方搭建沟通交流桥梁，增进网络空间及数据治理领域的对话与合作，在联合技术攻关、科技创新、产业化发展、上下游协同等方面开放合作，助力构建适应新型融合空间的国际规则和秩序，维护企业发展和国家利益。

孙　硕 | 北京市西城区委副书记、区长

孙硕在大会上介绍了西城区在推动网络安全行业发展的举措，包括积极开展多种形式网络安全知识教育、应急演练等活动，坚持打击网络攻击、电信网络诈骗等新型网上违法犯罪，不断筑牢网络安全社会根基。孙硕表示，西城区将进一步在以下几个方面推进网络安全和信息化建设工作。

首先是积极推进网络安全基础建设。西城区将致力于支持网络安全产业集聚创新。用好西城区“金服十条”“金科十条”“金开十条”及加快推进数字经济发展若干措施等政策，加快培育一批拥有网络安全核心技术和服务能力的优质企业。支持操作系统安全、新一代身份认证、终端安全接入等新型产品服务研发和产业化，建立可信安全防护基础技术产品体系。

其次是将大力培养引进网络安全行业领军人才。西城区将围绕人工智能、大数据、区块链、5G、工业互联网等领域优化资源配置，促进网络安全跨行业领域融合。

最后是着力培育网络安全优质产业生态。西城区将依托奇安信等龙头企业和一批知名投资机构，拟搭建全国网络信息安全创业投资服务联盟平台，构建网安行业生态、赋能创业企业成长，促进网络与信息安全企业健康快速发展。

奇安信
新一代网络安全领军者

补天漏洞响应平台

工业和信息化部网络安全技术应用试点示范项目

补天众测

网络安全漏洞领域唯一以安全厂商身份入选

企业商务合作请扫我

精英白帽子报名请扫我

官网：https://zhongce.butian.net　　邮箱：g-butian-deliver@qianxin.com　　公众号：补天漏洞响应平台

经营安全才能安全经营

—— 齐向东 BCS 2021 演讲全文

8 月 26 日，奇安信集团董事长齐向东在北京网络安全大会（BCS 2021）发表主题演讲时表示，DT 时代网络安全需要“动态掌控”，只有经营好安全体系，才能实现企业经营安全。

- ◎ 北京网络安全大会三年的主题共同组成了政府和企业实施网络安全的“三部曲”：理念、方法、动态掌控。
- ◎ 经营安全是对网络安全的动态掌控，只有让安全能力动起来，不断循环升级，才能破解复杂难题。
- ◎ 和时间同在，和变化同在，和运动同在，和安全同在。只要我们携起手来，共同经营好网络安全防线，就一定能迎来更富竞争力、万物生长的数字中国。

以下为奇安信集团董事长齐向东在 BCS 2021 大会上的演讲全文：

尊敬的各位领导、来宾，观众朋友们，大家好！欢迎参加第三届北京网络安全大会。

今天我的演讲题目是“经营安全 安全经营”。经营和安全，安全和经营，这两个词如果分开来看，很简单，每个人都会有自己的理解。但把它们放在一起，“经营安全 安全经营”这 8 个字，包含了思辨的逻辑关系和 DT 时代的价值观。

“经营安全 安全经营”，不是无源之水、无本之木。

回顾过去，2019 年，我们提出“内生安全”，把安全能力内置到信息化环境中，它是 DT 时代的安全理念；2020 年，我们提出“内生安全框架”，用系统工程的方法建成内生安全体系，它是内生安全理念落地的方法；今年，我们提出“经营安全 安全经营”，意思是，只有煞费苦心地经营你的安全体系，才能保障你的经营活动安全运转。

“经营安全”实际上是对网络安全的动态掌控。这三年大会的主题，共同组成了政府和企业实施网络安全的“三部曲”：理念、方法、动态掌控。按照这个三部曲的节奏去理解安全、实践安全、发展安全，未来我们生活的世界，必将出现万物生长的繁荣景象。

今天我提炼了两个关键词：DT 时代、动态掌控。

第一个关键词：DT 时代。

这几年，我们逐渐感觉到，时代正在发生深刻的变化。如何解读这种变化，决定了我们以什么样的方式去面对未来。

DT 时代的三大明显变化

第一个明显变化是，数据问题让国际关系变得越来越复杂。从欧盟颁布 GDPR 到推进数字税计划，从华为 5G、TikTok 被美国政府封杀到滴滴事件，我们可以明显感受到，世界各国对于数据主权的争夺越来越激烈，这种竞争在未来相当长一段时间都将是持续性的。

第二个明显变化是，数据资产成为了勒索攻击的头号目标。有人称勒索攻击成为了网络安全“流行病”，勒索的赎金越来越高，造成的威胁越来越大。今年以来，勒索攻击造成了断油、断肉、断播、断零售，赎金从 2000 万美元到 3000 万美元，再到 7000 万美元，屡创新高。

第三个明显变化是，针对关键基础设施数字化系统的攻击愈演愈烈。仅今年上半年，就发生了多起攻击事件，攻击对象包括美国自来水水厂、输油管道、南非港口、伊朗铁路的数字化系统，直接影响了人们的生活、社会的稳定和国家的安全。

这些变化，几乎都与数字系统和海量数据有关，标志着人类社会已经从 IT 时代进入了 DT 时代。

DT 时代的核心，是 D，data，也就是数据。数据是人的延伸、交易的延伸、服务的延伸；数据也带来了商业机会的延伸、生产力的延伸、想象力的延伸。数据本身是中性的，但是因为有不同的力量，站在不同的立场，以不同的方式来使用这些数据，数据就有了一体两面性。数据可以拿来做好事，数据也可以拿来做坏事。数据和人性一样，是非常复杂的。我们该如何与这种复杂性共生，是 DT 时代的一个重要命题。

DT 时代的三个显著特征

为了更好地理解这种复杂性，我总结了 DT 时代的三个显著特征。

第一个特征，企业经营者的安全责任，从以前的有限责任变成了无限责任。传统经济中，交易是“银货两讫”，交易结束后，企业经营者的责任基本也就结束了。但 DT 时代，几乎所有的交易都数字化了，一系列新技术、新应用、新场景和具体业务、具体用户结合在一起，共同构成了一个复杂系统。在这个复杂系统里，流动着复杂数据，发生着复杂交易。交易结束了，企业经营者的安全责任并未结束。

举个例子，以前，我们打车招手即停，到了目的地，交易就结束了；现在，我们用手机打车，产生了很多数据，即使出行结束了，用车平台仍然需要对我们的隐私、资金等各种数据的安全持续负责。最近，一位办企业的朋友向我咨询，员工违规违法导致数据丢失，企业要承担责任吗？我回答他：“数据泄露违法的锅，法人甩不掉。”企业法人的责任大小看两方面：一是后果，如果危害了

国家安全，责任就大了；二是看过程，如果企业没有按要求建设必要的网络安全系统，责任也就大了。这和传统的煤矿爆炸是一样的道理，如果矿场没有安全措施、制度和流程，那么矿主一定要承担主要责任。

可以说，只要用户的数据还存在，企业的责任就不会终结。保护每一个复杂交易的数据安全，成为了贯穿企业经营的生命线，是企业经营者的无限责任。

第二个特征，企业的经营活动，成为了国家网络安全的一部分。今年 7 月，滴滴上市第二天，网络安全审查办公室根据《国家安全法》《网络安全法》，对滴滴实行审查；7 月 10 日，《网络安全审查办法》修订草案公开征求意见，明确提出掌握超过 100 万用户个人信息的运营者赴国外上市，必须申报网络安全审查；8 月 17 日，国务院发布《关键信息基础设施安全保护条例》，明确行业主管部门、企业作为关键信息基础设施运营者要承担主体防护责任；8 月 20 日，《个人信息保护法》出台，明确了个人信息处理和跨境提供的规则……这一系列密集出台的法律法规充分证明，企业的经营活动已经和国家安全、社会安全发生了密切联系。

第三个特征，网络攻击破坏企业经营，变成了高频事件。今年 7 月，一家从事 IT 管理的软件服务商出现系统漏洞，牵连了全球上千家企业，受影响最大的一家零售连锁企业旗下的至少 800 家门店被迫停业；同样在 7 月，开源办公软件 Zimbra 爆出新漏洞，威胁了 20 万家企业的经营活动……这些网络攻击事件提醒我们，网络安全的威胁对经营活动的破坏力，变得如此巨大，难以承受。

DT 时代，无论是安全系统，还是经营活动，都具备了相当的复杂性。在未来相当长一段时期，想要安全经营，就要学会在经营中与这种复杂性打交道，这是生存和发展的关键。

所以，今年我们提出“经营安全 安全经营”。只有煞费苦心地经营你的安全系统，才能保障你的经营活动安全运转。

第二个关键词：动态掌控。

我今天演讲主题的第一句话是经营安全，在此之前，没有人把这两个词这样排列在一起。以前，我们提到网络安全，一般都说规划网络安全、建设网络安全、运营网络安全，还有网络安全运行。

那么，“经营”这个词，和以往有什么不同呢?

在 IT 时代，人们认为网络安全建设是一个简单活儿。IT 系统解决的是效率问题，如无纸化办公。IT 系统的部署场景是固定的，如政企机构的办公大楼。IT 系统解决安全问题的方法是隔离，不同的业务部门建设不同的网络，叫专网，在专网的边界上安装简单的安全产品。因此，IT 时代，网络安全公司的规模都比较小。

在 DT 时代，网络安全发生了颠覆性变化，变成了一个复杂活。DT 系统解决的是生产力问题，如数字经济，数据是生产要素，数据有生产、使用和交易问题。DT 系统是大数据架构的复杂系统，要拆墙、拔烟囱，靠安装简单的安全产品或者某种“银弹”，防住一切网络攻击是不可能的。DT 时代，安全变成了一个复杂的过程，先是通过运营发现问题，然后针对问题完善年度建设计划，之后再通过五年规划升级体系建设，让安全动起来，形成良性循环。总之，DT 时代，数据被泄密、篡改、删除、盗窃都是大事，网络安全对政企机构造成的影响，是巨大的甚至致命的。

所以，我们提出了“经营”这个词，经营安全是对网络安全的动态掌控，只有让安全能力动起来，不断循环升级，才能破解复杂难题。

实现动态掌控需要三个前提条件

◎ 经营安全的第一个前提条件是目标，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。在未来相当长一个历史时期，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势而动、因时而变、与日俱增的目标，也可以理解为用内生安全框架实现安全的弹性或扩展性。

◎ 经营安全的第二个前提条件是投入，要用足够的资源，来满足我们对安全无限的需求。

安全是没有性价比的，是以结果为导向的。DT 时代，网络安全成了“一失万无”的事，按照投入产出的因果关系，有投入才会有产出。这意味着，我们必须对安全有足够的资源投入。这个资源既包括钱，也包括人。工业和信息化部在《网络安全产业高质量发展三年行动计划（征求意见稿）》中提出，到 2023 年重点行业网络安全投入占信息化投入的比例要达到 10%。

◎ 经营安全的第三个前提条件是运营，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，尤其是在 DT 时代，边界消失，连接网络的终端泛化，给网络攻击者提供了充当伪装者的条件，攻击伪装者混在业务之中，很难一眼看穿。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。打个比喻，保障人身安全不能单靠个体的力量，还需要专业的警察来维护社会治安。在发达国家，把网络安全托管

给专业的安全公司来运营就非常盛行。

提升安全掌控力需要三个重要能力。

有了这三个前提条件，我们还需要三个重要能力，来提升对安全的掌控力。

经营安全的第一个重要能力，是认知能力。

强大的认知能力能够帮助人们把握事物基本规律、判断事物发展方向、构建自身与世界的关系。网络安全的认知能力也是如此，只有及时看到威胁、揪出威胁、阻断威胁，才能确保安全能力行之有效。

◎ 态势感知是建立认知能力的核心。2016 年 4 月 19 日，习近平总书记在全国网络安全与信息化工作座谈会上指出：“要全天候全方位感知网络安全态势。”总书记强调“没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是‘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’在里面，一旦有事就发作了。”

这几年，态势感知在我国发展很快，传统网络安全厂商和新兴的初创企业都在加大对态势感知的投入。我们总结，目前的态势感知主要分为三种：一种主要用于监管机构，我们称之为监管类态势感知；一种主要用于企业内网，我们称之为运营类态势感知；还有一种主要用于实战演练，我们称之为攻防类态势感知。

这三类态势感知，每一类单打独斗都不具备全面的认知能力。有的侧重互联网宏观态势的监测，缺乏针对性；有的侧重日常的安全运行维护，缺乏攻防能力；有的侧重战时的攻防对抗，缺乏平时常态化的运营。更为突出的问题是，只看局部不看整体，有的没有覆盖生产业务系统；有的没有覆盖三级、四级末端的网络；有的没有覆盖物联网、云、数据库和计算平台。

只有将这三类态势感知有机协同在一起，形成实战化态势感知，才能全面提升认知能力。三类态势感知能有机协同，需要构建统一的计算平台、标准和运营系统。有人把态势感知等同于安全大脑，这是不全面的。它是大脑（包括五官）、四肢和武功的三合一。大脑是监管态势，能看见威胁；四肢是运营态势，能揪出威胁；武功是攻防态势，能阻断威胁。

◎ 认知能力的关键是安全运营。就像人的认知能力来自学习和实践，网络安全的认知能力来源于实战攻防的运营，通过运营实现攻击告警、调查溯源、拦截阻断的往复循环。

◎ 安全运营的基础是资配漏补。资配漏补是资产、配置、漏洞和补丁的统称。先要把软件、硬件、协议等资梳理清楚，建立档案，用系统管起来。在网络安全攻防中，人是战斗的士兵，资产就是城池。如果自己有多少城池都不清楚，做出的网络安全规划一定是不全面的。只有把自己的资产地图画出来，网络攻防战才能有规划、有打法；我们还要做好配置管理、漏洞管理和补丁管理。只有当资配漏补都做好了，我们才能发现安全产品的不足和安全体系的缺陷。日积月累下来，不合格的产品会逐渐退出，合格的产品会越来越好，安全体系会越来越健全。

经营安全的第二个重要能力，是安全能力。

以前，我们把安全市场分为产品市场和服务市场，产品和服务是两回事。现在，要把产品变成一种能力，把能力变成一种资源，并用服务的方式使用资源。换句话说，把安全产品能力化、资源化、服务化。

◎ 安全产品能力化，首先要把安全的硬件产品软件化。这是一个艰巨的任务，因为过去为了降低成本，往往选用配置较低的硬件平台。同时，为了提高性能，往往把软件和硬件平台深度耦合。所以，

把软件从专属的硬件平台上抠出来，适配更通用的硬件平台，几乎需要对代码重构、重写。

◎ 安全产品资源化，首先要实现数据和 API 标准化。各种各样的安全产品从数据采集、治理、存储、分析，到结果输出使用、API 服务，都应该遵从统一的标准，更要与网、云、数据、应用的标准对接。这样，客户就可以用一朵安全云，把所需要的安全产品以资源的形式纳入其中。安全能力资源对外服务过程中产生的日志，自然就形成了安全大数据，可以据此推出能提供更多安全能力的安全大数据中台服务。

◎ 安全产品服务化，首先要做到调度指挥。把安全能力以资源服务形式嵌入到需要的每个角落，并且这种安全能力的质量是可评估的。例如，发生网络攻击的当时没有告警，但事后通过分析溯源，定位出是防火墙漏掉了这次攻击，我们就会去改进防火墙技术，或者用资源服务的方式快速地换用其他家的防火墙。

这种安全能力服务，还便于商业模式创新。以前我们采购安全产品，通过招标确定供应商，一经选定之后，就没有机会使用其他品牌的产品了。安全能力资源服务的形式，可以选定多家安全公司的产品部署在安全云上，不使用不付费，依据使用的多少来结算。购买产品模式拼的是商务关

系和测试方案，而能力资源服务模式拼的是实战效果，这种模式更能推动厂家技术创新。

经营安全的第三个重要能力，是授信能力。

◎ 网络安全的核心问题，是信任问题。比如，Wintel 体系不是可信计算，所以有很多计算机病毒出现。沈昌祥院士推出的可信计算技术体系，能免疫 Wintel 时代的病毒。中国电子推出的 PKS 体系，是飞腾 CPU、麒麟操作系统融合了可信华泰的可信计算及奇安信的安全技术。

◎ 另一方面，网络除了计算，更多的是人机交互，人是安全最大的变量，人的可信度成了难题。还有，数据变成生产要素之后，谁在什么场景、用于什么目的、可以使用什么数据，也变成了一种授信问题。

◎ IT 时代的授信能力是粗放的和不足的。假设我们把每一次的网络访问都分为主体（访问者）和客体（被访问者）。主体有很多，如人、IoT 设备、App 应用等；客体也有很多，如业务系统应用、云计算资源、接口、数据资源等。在传统的认证体系里，授信是比较粗放的，一个主体可以访问多个客体，一个客体也可以允许多个主体访问。这种方法有很多漏洞，广泛地被黑客利用进行攻击。

◎ DT 时代的授信能力是零信任体系提供的，通过动态评估信任实现动态可控。它不再绝对信任任何一个主体，而是给每个主体、每个客体附加很多属性，以“权限最小化”原则进行授信，并且对授信持续进行动态评估。比如，账号 A 是个主体，它的属性包括机器指纹、网络类型、IP 地址、使用时间、工作职责和机器环境。再如，数据资源 B 是个客体，它的属性包括类型、敏感级别、来源、机密、隐私、连接关系、各种标签等。以“权限最小化”原则，我们授权“A 在办公室网络下、在专项工作期间，可以访问非机密属性的数据资源 B”。一旦发现 A 的办公室网络属性消失，或者专项工作的属性消失，这个授信就自动取消。整个过程都是通过系统自动动态评估完成的。

◎ 这种授信能力是网络安全的保障。我在《漏洞》一书中提出网络安全的“四个假设”即“假设系统一定有未被发现的漏洞、假设一定有已发现但仍未修补的漏洞、假设系统已被渗透、假设内部人员不可靠”。

关于内部人员对网络安全的危害程度，我在《漏洞》一书里也有披露，“85% 的网络攻击源于内部”。这个“源于内部”和“内部人员”是一回事，它包括人被收买、账号被盗用、机器被利用、供应链被后门等，之所以被攻击成功，就是因为我们对自己的人、自己的账号、自己的机器、自己的认证、自己的供应商过度信任。

结语

总结起来，DT 时代的网络安全是一件复杂的事，只有经营安全，才能实现对网络安全的动态掌控，而动态掌控力的提升有赖于三种能力：认知能力、安全能力和授信能力。

一位古希腊哲学家提出过一个著名的悖论，叫作“飞矢不动”。说的是把一只短箭射出去，它在空中飞行，它是运动的。但是如果把时间切割开，单独去看每一个瞬间的短箭，它是一样的，好像并没有运动。

“飞矢不动”的悖论告诉我们一个道理，静止是相对的，运动是绝对的。安全也是一样，它看不见摸不着，但是当网络攻击发生了，我们也就感受到了安全的存在。

这也是我今天提出在 DT 时代，“经营安全 安全经营”这 8 个字的用意。和时间同在，和变化同在，和运动同在，和安全同在。我相信，只要我们携起手来，共同经营好网络安全防线，就一定能迎来一个更富竞争力、万物生长的数字中国。谢谢大家！安

奇安信

新一代网络安全领军者

奇安信营销体系

招募精英

党政大客户部总经理

1.负责中央部委及二级单位市场的全年销售任务达成；
2.制定年度销售计划及预算，分解销售任务，推动并确保相应计划、目标的达成；负责团队的建设、管理、指导与激励；
4.重要客户中高层关系维护，项目运作与把握；潜在客户的市场拓展，制定增量目标，计划并达成；
5.进行市场调研与分析，研究同行业界发展状况，为公司战略制定、产品规划等方面提供相应建议。

大客户销售经理

党政/网信/电子政务/审计行业

1.根据公司及本行业销售任务开展销售工作，完成各项销售指标；
2.开拓、积累、夯实客户基础；
3.挖掘客户需求，为客户提供整体解决方案；
4.负责组织开展行业市场活动，加强公司在行业内的品牌影响力；
5.挖掘、反馈所负责行业的市场信息及客户需求，促进产品体系优化，构建有竞争力的市场策略。

售前技术专家

党政大客户部

1.负责国家党政机关头部客户的售前技术工作，协同党政大客户部销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求
2.负责党政大客户部客户技术交流、项目技术文档编写、项目招投标等售前支撑工作；
3.负责党政大客户部技术策略梳理、技术资料整理，并能在党政机关头部客户进行技术和解决方案推广。

解决方案专家

党政/网信/电子政务/审计行业

1.协助行业技术负责人完成行业级解决方案、营销技术策略、行业技术资料整理，并能在行业进行技术和解决方案推广；
2.协同行业销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求；
3.完成行业市场典型客户调研，不断提升解决方案竞争力，能洞察行业趋势、参与行业规范制定。

扫码联系我们

新京报

8 月 26 日

DT 时代责任无界 经营安全才能安全经营

8 月 26 日，2021 北京网络安全大会（简称 BCS 2021）以云峰会形式盛大启幕。大会的主题为“经营安全，安全经营”，大会联席主席、奇安信集团董事长齐向东指出，DT 时代网络安全需要“动态掌控”，只有经营好安全体系，才能实现企业经营安全。十余位两院院士，200 多位全球重磅嘉宾，围绕安全责任、产业趋势、数字城市、数据治理、车联网、密码应用等热点议题展开交流讨论。BCS 被称为网络安全领域的达沃斯，近三年的大会主题词“内生安全”“安全框架”“经营安全”，共同组成了政府和企业实施网络安全的“三部曲”。

原工业和信息化部党组成员、副部长刘烈宏，北京市委常委、副市长殷勇，中国电子信息产业集团董事长芮晓武，十三届全国政协委员、社会和法制委员会副主任，中国友谊促进会理事长陈智敏，中国网络空间安全协会理事长王秀军，中央网信办网络安全协调局局长孙蔚敏，工业和信息化部网络安全管理局局长隋静，公安部网络安全保卫局一级巡视员、副局长郭启全，北京 2022 年冬奥会和冬残奥会组委会副秘书长徐志军，全国工商联副秘书长、会员部部长郭孟谦，北京市西城区委副书记、区长孙硕，北京市委网信办副主任侯健美，北京市经信局副局长顾瑾栩等领导出席并致辞。

DT 时代 企业需与复杂性共生

齐向东在大会上表示，当前我们已进入 DT（Data Technology）时代，网络安全形势非常严峻复杂，网络攻击威慑上升。数据成为重要资产，世界各国对于数据主权的争夺越来越激烈，直接影响国家安全和国际关系。高级持续性威胁、数据窃取等事件频发，网络勒索已成数字世界的“流行病”，针对关键信息基础设施数字化系统的攻击愈演愈烈，危害经济社会稳定运行。

海量的数据，一方面为社会带来了便捷和效率，另一方面却给企业经营者带来了无限责任：传统社会中，交易或服务完成后企业的责任即解除，DT 时代由于数据存储而转变为资产，企业的责任无法终结。甚至企业的数据安全直接成为国家安全的一部分，网络攻击破坏企业经营已成高频事件。

基于上述现实，BCS 2021 将今年的大会主题定为“经营安全 安全经营”，提出网络安全发展迎来新拐点，社会进入数据驱动新阶段，网络安全已成为数字化发展的前提。安全就是生产力，就是竞争力。网络安全已经从成本转变为生产力，面对数字化的网络安全高要求及风险的高度不确定性，网络安全需要改变发展思维和发展模式。DT 时代，无论是安全系统，还是经营活动，都具备了相当的复杂性。在未来相当长一段时期，想要安全经营，就要学会在经营中与这种复杂性打交道。只有煞费苦心地经营安全系统，才能保障经营活动安全运转。

齐向东谈到，经营安全是对网络安全的动态掌控，只有让安全能力动起来，不断循环升级，才能破解复杂难题。要做到经营安全，首先要让安全能力与日俱增，

原工业和信息化部副部长刘烈宏

保护复杂系统和复杂交易。安全没有性价比，安全“一失万无”，要用足够的资源，来满足我们对安全无限的需求；要用专业高效的安全运营服务，来抵御复杂的网络攻击。

多重政策叠加利好网络安全行业提速发展

根据工业和信息化部今年编制《网络安全产业高质量发展三年行动计划》，到 2023 年，我国网络安全产业规模超过 2500 亿元；电信等重点行业网络安全投入占信息化投入比例不低于 10%。在 2500 亿市场的加持下，中国网络安全产业正迎来全面提速发展。

原工业和信息化部副部长刘烈宏在致辞中表示，党中央、国务院高度重视网络安全工作，面向建设网络强国、制造强国、数字中国作出一系列重大决策部署。工业和信息化部认真贯彻落实这些决策部署，大力推动网络安全产业创新发展，取得积极成效。2021 年通过部署 5 项重点行动计划、设立 4 项重点工程，促进我国网络安全产业综合实力再上新台阶。

北京市委常委、副市长殷勇在大会上表示，近年来，北京市大力推进国家网络安全产业园区建设，积极培育网络安全企业集群，网络安全产业呈现出产业规模领先、产业链结构完整、产业生态完善的良好发展态势。未来，北京市还将从发展数字经济、支持产业聚集，探索建立数据安全管理体系、优化营商环境等四方面，推动网络安全产业高质量发展，努力建设全球数字经济标杆城市。

大会名誉主席、中国电子信息产业集团有限公司董事长芮晓武指出，数字化、网络化、智能化融合发展，网络安全产业也迎来融合发展的新趋势。中国电子与奇安信携手，作为网络安全和信息化产业国家队，将加快推动可信计算技术融入先进计算架构、加快推动网络安全防护融入信息系统建设、加快推动生态体系建设融入

北京市委常委、副市长殷勇

大会名誉主席、中国电子董事长芮晓武

产业发展进程，通过三个“融入”举措，推动网络安全产业融合发展。

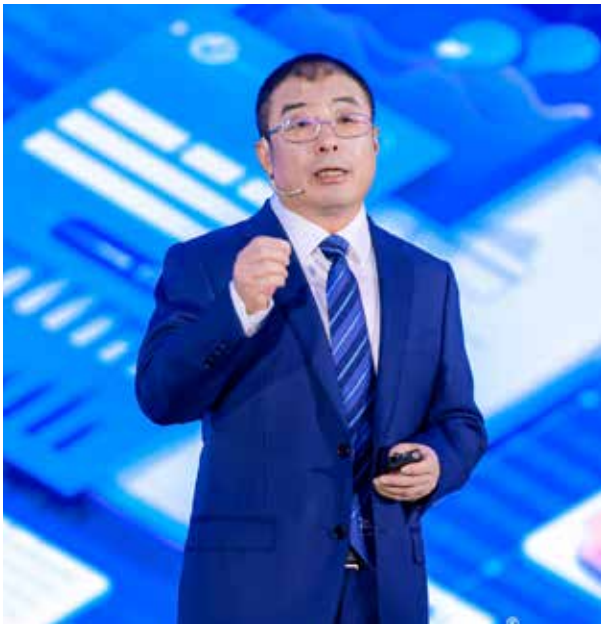
十三届全国政协社会和法制委员会副主任、公安部原副部长、中国友谊促进会理事长陈智敏对大会表示祝贺。他指出，数据是网络安全的生命线，没有数据安全，就没有网络空间安全，没有网络信息安全，也没有网络信息基础设施的安全。切实保护好数据安全，不仅要加强政策、监管、法律的统筹协调，还需要从理论上、法律上进一步解决数据权属问题。陈智敏在会上提出了解决数据权属问题的九项基本原则，为 DT 时代的安全经营提供了权威的准则参考。

俄罗斯前副总理谢尔盖 · 沙赫赖通过远程连线参加本次大会。他表示，网络安全已经成为国家和社会的主要安全问题，在世界范围内新冠肺炎疫情肆虐的背景下，每个国家都能够特别敏锐地感受到数字和信息通信的脆弱性。中、美、俄三个国家之间的密切合作和原则性共识，对于顺利推动和达成全球网络安全目标至关重要。希望建立中、美、俄高层的定期线上会晤机制，划出不得逾越的红线，构建国际网络安全体系。

“从 2019 年到 2021 年，北京网络安全大会三年的主题，共同组成了政企机构实施网络安全的‘三部曲’：理念、方法、动态掌控。”齐向东谈到，按照这个三部曲的节奏去理解安全、实践安全、发展安全，未来整个产业，包括我们生活的世界，必将出现万物生长的繁荣景象。

3+18+N 系列活动 24 小时直播奏响网安行业最强音

围绕“经营安全 安全经营”等话题，参加 BCS 2021 的专家将展开为期 3 天的讨论，呈现战略峰会、产业峰会、技术峰会三大主题峰会和 18 场系列活动。受新冠肺炎疫情影响，大会的所有会议和活动将全部进行网络直播，并结合“安全小姐姐”“BCS 会客厅”“名人名书”等 N 个特色线上栏目，形成 24 小时不间断的网络安全直播盛宴。同时，本届大会还首次引入“XR”直播技术，让观众感受身临其境的观看体验。届时，网友



北京网络安全大会联席主席、奇安信集团董事长齐向东

图：近 200 家企业入住 BCS 2021 云展厅

将可以通过大会官网、H5、微信视频号、抖音、B 站等多种不同平台进行观看。

BCS 2021 还为参会企业、机构和观众专门开发了线上展览展示平台，有近 200 家企业入住参展的 3D 云展厅，设有护航冬奥馆、核心动力馆、安全科技馆、安全创客汇、补天白帽馆等十余个主题展馆。作为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，奇安信集团邀请了多位冬奥神秘嘉宾，包括速滑世界冠军宁忠岩、单板滑雪世界冠军蔡雪桐等。组委会还邀请到了 12 家冬奥赞助商、供应商在 3D 云展厅亮相，观众可参与线上互动，领取积分兑换好礼。

“全球网络安全，倾听北京声音。”本次会议吸引了全球顶尖学者、技术专家、行业领袖、产业精英，带来了网络安全领域前沿资讯及思想碰撞。俄罗斯前副总理谢尔盖 · 沙赫赖，特拉维夫大学安全研究项目负责人本 · 以色列，美退役陆军少将、Palo Alto Networks 全球副总裁兼首席安全官约翰 · 戴维斯，发现 WannaCry 关闭开关而阻止勒索软件的进一步传播的英国安全研究员 Marcus Hutchins，美国俄克拉荷马大学研究和合作伙伴关系副总裁 David S. Ebert 等国际范围内的知名网络安全专家、学者也将受邀出席大会并发表演讲。Gartner、Forrester、IDC、德勤四大国际第三方机构亮相，也将带来权威、客观的行业分析及前沿观点。安

TechWeb
www.techweb.com.cn

本·以色列：揭秘以色列网络安全产业生态的发展之路

特拉维夫大学安全研究项目负责人本·以色列连线2021北京网络安全大会战略峰会开幕式，并发表线上演讲。他表示，以色列是世界上第一个承认网络技术，使其成为民间社会的合法职业的国家，起因是19年前他写给时任以色列总理的一封信。

在2010年之前，以色列网络安全仍然由情报和国防部门主导，是绝对保密的。突然有一天，有人通过网络袭击了伊朗的铀浓缩离心机。在那一周内，全世界都在谈论网络安全问题，因为攻击者在没有使用炸弹的情况下破坏了铀浓缩设施，而且这是首次向公众展示在网络空间发生的、给真实世界造成实质性损失的网络攻击案例。

随后，以色列总理召见了本·以色列，因为其在90年代写给当时首相（也就是前任首相）的一封信。信中本·以色列曾表示，总有一天全世界都会见识到网络技术的潜力。以色列的信息化程度非常高，几乎所有的关键基础设施都被计算机控制了，而不是由人类控制。一旦每个人都明白了这个道理，他们就可以通过控制计算机来破坏系统。

正因为1999年的这封信，以色列政府在2002年成立全新的负责关键基础设施网络安全的政府机构。2022年，这项网络安全防护体系即将建成20周年。

本·以色列认为，安全不仅仅是指技术安全，在21

世纪，我们面临的大多数问题，其源头往往来自于人性，如果你不了解法律问题、商业考量、个人心理，以及整个社会的大众心理，就无法真正理解问题的本质。因此，本·以色列提交给政府的计划中要求建立完整的生态系统，不仅涉及技术、大学、教育，而且还涉及行业问题、待要解决的法律问题、以及伦理道德问题等。

本·以色列表示，以色列目前的情况比他十年前预计的要好得多。从经济角度来说，以色列的网络安全产品和服务几乎占了世界市场份额的10%。在网络安全投资方面，以色列的份额从2018年的18%，上升到2020年的31%，目前2021年上半年比例已经达到45%，在商业机构得到的投资已经超过了排名第二的美国。可见，以色列当前蓬勃发展的网络安全产业，得益于良好的网络安全生态土壤和全民意识基础。安

战略热点

俄罗斯前副总理：两条规则保障网络安全

俄罗斯前副总理谢尔盖·沙赫赖受邀出席 2021 北京网络安全大会 (BCS 2021) 开幕式 & 战略峰会，并发表了致辞，他表示，网络安全已经成为国家和社会的主要安全问题，这是当代国际法要面对的一个关键问题。

自 1998 年以来，关于国际法作用的讨论一直是联合国网络安全议程的一部分，各国不断讨论国际法在网络空间的适用领域和界限；2009 年 12 月 21 日，联合国大会决议中强调，安全而放心地使用信息技术是信息社会的一大支柱；2013 年，15 个国家的代表一致同意，包括《联合国宪章》在内的国际法也应该适用于信息和通信技术领域，这对于保持和平、稳定、开放、安全、可访问的信息通信环境是很有必要的。

谢尔盖·沙赫赖表示，过去 30 年，国际层面上进行了各种各样的尝试，以期在界定网络空间监管、网络安全保障的原则方面达成共识。他指出，只有受保护的数字主权国家才能够有效地保护生活在其疆域内的民众，因此全球趋势是“数字空间的主权化”。

谢尔盖认为，中、美、俄三个国家之间的密切合作和原则性共识，对于顺利推动和达成这一目标是至关重要的。这三个国家与其他国家不同，它们已经初步构建了法律和技术能力，以保证自身享用充分的“数字主权”，统计数据也可以很好地验证这三个国家对“世界政治气候”的重要性。专家们认为，“俄罗斯 – 中国 – 美国”三角关系复杂且相当紧张，这是威胁整个世界的潜在冲突根源，但他坚信解决几乎所有当代全球问题的钥匙也恰恰蕴含在这个三角关系中。

谢尔盖·沙赫赖建议，当前，中、美、俄三个主要世界大国的高层需要加强会晤。首轮“三方”会晤机制应该聚焦于网络安全问题，因为这是能启动三方高层定期会晤的最为重要的议题。同时，还应当划出不得逾越的红线，使各方不能发明任何新方法，以真正有远见的美国科幻作家艾萨克·阿西莫夫提出的著名定律为出发点。这个机器人学定律极其简单且众人皆知，同时这个定律也包含着大量的伦理道德因素，这些因素是构建人类与其智慧结晶——计算机之间的全新社会契约的哲学基础所必须具备的。

除此之外，谢尔盖·沙赫赖还提到保障网络安全的两条规则：一是公约缔约国须承诺其控制论系统 (Cybernetics) 不会因自身的作为或不作为而伤害人类；二是在不违背基本规则的前提下，公约缔约国有权采取一切措施来确保自身网络安全并独立发展本国的网络系统。

最后，谢尔盖·沙赫赖提议：“为了保护网络空间中的人类生命，我们应该共同制订并缔结《网络安全基本法全面公约》”。安

赛迪网 CCIDNET.com

约翰·戴维斯：全球勒索攻击近乎“失控” 抗衡需国际协同合作

观潮论坛海外联合发起人、Palo Alto Networks 全球副总裁兼首席安全官约翰·戴维斯（John Davis）出席 2021 北京网络安全大会（BCS 2021）开幕式 & 战略峰会，发表题为《战略调解的新探索——为更大的全球合作寻求解决方案》的演讲。

约翰·戴维斯指出，当前世界各地都不同程度的遭遇过勒索软件攻击，这场大规模的“数字流行病”正在影响包括学校、警察局、政府部门，以及医院和交通网络，未来或波及蔓延至 5G 网络领域。

2021 年 1 月，约翰·戴维斯开始担任由美国安全与技术研究所资助的国际勒索软件任务组联合主席。任务组是由政府、企业、非营利组织和学术界的 60 多名专家组成的公私合作组织，旨在通过一系列行动破坏勒索软件的商业模式。

2021 年 4 月，任务组发布报告，就如何预防与应对勒索攻击给出四项建议：一是通过国际组织制定的综合战略预防阻止勒索软件的攻击；第二是打击勒索软件的商业模式、降低犯罪所带来的盈利；第三是帮助各类组织做好应对勒索软件攻击的准备；四是更快速地应对勒索软件的攻击。

约翰·戴维斯表示，勒索软件对于全球网络的威胁程度正在不断攀升。传统的应对方式过于分散，无法有效地应对勒索软件。因此，任务组建议采取极限施压的策略，以统一的标准，从 “威慑、瓦解、准备、响应”四个方面压制勒索软件。

其中，威慑（Deterrence）是指各国政府应发布统一的外交声明政策，建立国际联盟打击制造勒索软件犯罪分子；瓦解（Disruption）则是通过使用各种适用于国家和国际的能力要素，瓦解勒索软件制造者对于基础设施和支付环境的破坏；准备（Preparation）则是建议国际社会需建立最佳标准的实践框架，以缓解、应对勒索软件的攻击；响应（Response）是指国际社会应统一勒索软件信息和勒索事件报告的标准形式，把勒索软件攻击报告作为一项公益事业。

约翰·戴维斯强调，勒索病毒是国际社会面临的共同威胁，无论是公共部门还是私营组织，都没有足够的能力、技巧、知识、资源与勒索攻击单独抗衡。需要由政府、企业、学术界、非营利组织和其他领域组成联盟团队，通过国际协同合作对目前近乎于“失控”状态的勒索病毒实施有效控制管理。对于国际社会而言，抵御勒索软件符合全球共同利益，也是确保 5G 和物联网发展的基石。安

经济参考报

郑永年谈网络世界“两极化”与安全发展

香港中文大学（深圳）全球与当代中国高等研究院院长郑永年出席 2021 北京网络安全大会 (BCS 2021) 开幕式 & 战略峰会，并发表《网络的“两极化”及一个不安全的世界》主题演讲，站在当前世界各国面临的安全问题角度，阐述网络安全的多重可能性。

郑永年指出，从农业社会到工业社会，直到现在的信息社会，社会面临的安全是不一样的。在互联网时代、信息时代，社会面临着越来越严峻的安全考验。未来世界各国之间的真正战争，也将会是网络黑客构建的结果。

可以说，网络安全是当今世界各国之间交流的重要议题，与每一个人的生活都息息相关。一旦网络遭到攻击，无论是个人、家庭，还是公司、学校等社会各行各业，乃至国家都会受到重大影响，这就是“没有网络安全就没有国家安全”。

郑永年强调，从观察结果来看，不同国家对网络安全表露出来的态度也是不一样的。以美国为例，作为拥有世界顶尖网络技术和人才的国家，却总是将自己塑造成受害者形象，指责其他国家对其发动网络攻击；相比美国，俄罗斯对此态度更加开放，将网络攻防水平视为国家实力的重要部分。

站在国际关系层面，郑永年认为未来的网络世界存在以下五种可能性：

第一种，受国家之间的竞争关系影响，网络空间同样彼此割裂、互不来往，我们面对的情况就是互联网向“互不联网”转变；

第二种，国家间的网络世界并不完全脱钩，但可以互相威慑，这需要国家具有足够的网络对抗实力，这种威慑与现实世界中的“核威慑”类似；

第三种，世界各国不断拓展自己的互联网空间，逐渐形成以大国为中心的区域网，造成多中心的网络世界局面；

第四种，多元化的互联网世界，网络世界未来发展未必会迈入两极化，而是随着互联网的不断发展创新，形成多元化的网络系统互相制衡；

第五种，是基于主权国家之间合作和政治信任之上的互联网世界，国家之间达成信任共识，网络空间形成互相开放、互相合作、互不攻击的局面。

从上述几种网络世界发展的可能性来看，网络安全形势仍然不容乐观。郑永年认为，在互联网空间发展的道路上，世界各国均面临着重大选择，需要理性讨论网络安全问题，共同建设安全的世界互联网体系。安

鳳凰網科技

中外专家汇聚 BCS 共商数字世界竞合之路

2021 北京网络安全大会（BCS 2021）暨第六届观潮论围绕数字世界的竞合之路展开对话。本次观潮论坛由国家创新与发展战略研究会（以下简称国创会）和奇安信集团共同主办，面对技术垄断、国家数据主权、关键基础设施安全、勒索攻击等难题，中外专家直击脱钩对抗的问题痛点，寻找合作共赢的对策解药，为更大的全球合作寻求解决方案。

观潮论坛主席、国创会副会长郝叶力表示，中美总体上应是竞合范式。数字经济“分享、再生、创造”的特点提供了一种普惠包容的发展模式，应引入“新变量、新视角、新格局”，避免全球新冷战。中美有着共同引领全球经济通过数字化增长摆脱困境的历史责任，应重视全球数字经济的流域特点，用“增量思维，整体思维，流域思维”，以创新模式破解区域发展不平衡，维持地球生态与可持续发展，尊重多元化体制选择，走向“数字融合的世界”。

观潮论坛理事长、奇安信集团董事长齐向东表示，疫情没能阻止我们对网络安全的关注和思考，数字技术开辟出的新世界带来了无数机遇，但与此同时，数字世界超越了虚拟空间的局限，频频发生的勒索攻击对人民生活、企业生产、社会稳定和国家安全造成了难以估量的危害。在数字世界里，有合作才有未来。这就需要各国政府、学界和产业界联合起来，把合作共赢放在第一顺位，积极寻找利益契合点，运用数字技术解决共同的难题，最终合作的硕果将惠及本国、惠及全人类。

联合国经济和社会事务部公共机构和数字政府司司长朱巨望在线上参与论坛讨论说，“公平竞争、合作共赢是推动全球可持续发展、数字世界普惠全人类的必由之路，互联网和数字世界的治理是全球人类共同的使命。”目前，联合国也在深入探讨数字技术与和平安全、数字转型与可持续发展、预防网络犯罪等问题，就数字世界的未来制定网络空间贸易规则。

美国退役陆军少将、Palo Alto Networks 全球副总裁兼首席安全官约翰 · 戴维斯组建了专门的任务组应对肆虐全球的网络勒索。他呼吁世界各国把勒索软件当作其执法重点，建立国际联盟，搭建勒索软件调查中心的全球网络，通过国际协调的综合战略阻止勒索软件攻击，瓦解勒索软件的商业模式，帮助各组织为勒索软件攻击做好准备，更有效地响应勒索软件攻击。

俄联邦安全会议第一副秘书奥列格 · 弗拉基米罗维奇 · 赫拉莫夫上将说，“任何一个世界大国都无法单独应对跨境信息领域中存在的种种威胁，在该领域发展合作是客观需求。”他建议各国建立在全球信息空间活动的国际法原则规范，为联合国通过《国际信息安全公约》创造条件，建立因特网安全稳定运行与发展的保障机制，尽快签署各国不首先使用信息通信技术相互攻击的协议，实现联合调查网络欺诈和勒索犯罪案件。

新加坡亚洲区块链产业研究院院长陈柏珲指出，每一次重大的科技发展都进一步推动全球的经济发展与一体化，疫情之后的世界，需要科技发展与合作来推动世界经济融合发展。中美双方在网络安全、应对气候变化等众多议题上面都有合作的空间，应该让贸易与科技问题回归竞争与合作的本质，保持开放，共同面对挑战。

厦门大学台湾研究院讲座教授、战略与安全研究中心主任郑剑提出，经济和战略是推动国家对外政策制定与实施的两大最强有力的引擎，经济力与战略力的平衡与失衡是大国兴衰蕴藏的逻辑密码，中、美两国亟须寻找更稳健的大国关系的平衡点。

复旦大学国际问题研究院副院长、俄罗斯中亚研究中心主任冯玉军认为，国际大变局下，世界发展的不平衡性进一步增强，呈现出非线性的“畸变”。新能源革命、新技术革命和新知识革命正在深刻地影响着世界格局的变化，国际格局、世界秩序和大国关系正在呈现出一种进一步复杂的趋势，中、美、俄等大国应把握多重变奏，形成战略稳定新框架。

国家发展改革委产业经济与技术经济研究所原所长、研究员黄汉权提出，当前大国博弈主导下，技术民族主义再现，应客观认识其利弊。技术创新和全球化是各国经济增长的主要驱动力，自由竞争和开放合作是科技创新最好的土壤。把握自主创新与开放合作的平衡点，推动中美数字世界合作。

业界专家刘松认为，中美科技竞争总体弊大于利。科技人才协作和供应链断裂将阻碍科技基础研究的进步与产业化，导致数字科技与数字经济的普惠包容特点无法帮助整个世界更多的中低收入群体、中小企业的发展，最终让世界经济的增长遇到更大的挑战。数字科技是对世界整体发展有利的增量推力，不应以武器思维看待数字技术。数据、人才和知识的流动不能被割裂，应该以“多方参与 + 多元治理”寻找数字动能的创新增量、数字治理的协同可能、数字安全的行为底线，避免冷战思维意识形态化和技术民族主义。

华为战略部高级专家乔维则认为，数字空间和现实空间的融合对全球数字治理提出了挑战，亟待建立适应新型融合空间的国际治理体系。AI 治理、数据治理及网络空间治理等新型治理问题需要各国政府、NGO、智库、企业、学术组织之间多方协同，通过新的治理体系维护数字时代的全球秩序，保障全球供应链安全。安

2021 北京网络安全大会系列活动启动仪式上，三位 2008 年北京奥运会火炬手，与四位中国工程院院士、相关主管部门领导，和奇安信集团董事长齐向东一起，共同宣布了网络安全中国代表队的正式组建。


中国代表队
中国代表队
奇安信
CHINA
速度滑冰世界冠军
奇安信品牌代言人
宁忠岩

吴云坤：网络安全的新范畴、新管理、新模式和新范式

8 月 27 日，奇安信集团总裁吴云坤在 BCS 2021 产业峰会发表主题演讲时表示，网络安全迎来了新的拐点，需要通过新范畴、新管理、新模式和新范式，将网络安全挑战转化为机遇。

- ◎ 从先发展后治理、同步发展和治理到治理先行，这是从信息化视角看网络安全的巨大转折，网络安全迎来了发展新拐点。
- ◎ 在数字化时代的网络安全新征程上，网络安全从业者要主动转换新角色、发展新能力、共建新生态。
- ◎ 内生安全框架就是通过工程化的方法，通过十大工程和五大任务来满足各种需求，帮助客户搞好建设、做好运营，满足各种法律法规要求。

以下为奇安信集团总裁吴云坤 BCS 2021 产业峰会演讲全文：

尊敬的各位嘉宾，各位新老朋友，上午好！

很高兴能在每年的这个时刻、在这个平台上，跟新老朋友们一起观察、思考和判断产业发展环境和产业发展方向。就像去年 BCS 大会上我提到的，产业环境就是我们的生存环境，它是池塘、河流还是海洋，将直接决定着我们的发展空间；产业方向则引领我们的发展思维

和行动方略。

今天的演讲题目是“网络安全产业的新拐点与新征程”。“新拐点”是对“十四五”期间产业环境的判断，“新征程”是探讨在新拐点上我们应该怎么干。

第一部分：网络安全迎来发展“新拐点”

回顾网络安全发展过去的 25 年历程，有人说是合规驱动，也有人说是威胁驱动，但如果我们回到一个主脉络，就会发现网络安全的发展其实是跟信息化的发展及信息化对业务的影响紧密相关，这才是发展的主脉络：随着信息化对业务的重要性越来越大，威胁也会逐步升级，合规监管也日趋严格，网络安全产业的增长速度随之越来越快。

1995-2004 年，信息化对于业务是辅助性的，网络安全也处于非常初级的阶段：发展很慢，规模很小，每年只有几十亿规模，十年间复合增长率只有 5.8%。

2005-2014 年，信息化开始跟业务结合，网络安全也随着合规和威胁升级变得越来越重要。安全问题开始显性化，如政府网站被控影响国家安全；企业财务系统感染病毒会影响生产经营。在等保合规和应对威胁驱动下，网络安全产业开始加速，年产业规模开始超过 250 亿，10 年间复合增长率也超过了 10%。

在这阶段网络安全的整体思路还是先发展后治理。

2015-2020 年，随着全面数字化转型，信息化与业务深度融合，信息系统的安全与业务稳定运行高度相关。

黑客组织也发现了信息化对业务系统的影响，采用更加高级的手段对信息化系统进行攻击，如 APT 组织攻击重要系统，窃取关键业务数据或机密信息。

2014 年，习总书记提出了“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”。国家先后出台了《国家网络安全战略》和《网络安全法》，完成了网络安全的顶层设计。

以《网络安全法》为核心开始建立和健全网络安全法律法规、标准规范、监督检查机制等网络安全治理体系。

这一阶段的发展思路是同步发展同步治理：在信息化发展的同时开展网络安全治理。

2021 年开始，随着“十四五”的到来，数字化已经开始贯穿于经济社会发展的全领域、各层级，成为国家治理、经济发展和社会运行的核心驱动力，数字化对于国家、企业和每个人都真正是生死攸关。

因此，国家在“十四五”规划中提出数字化发展战略的同时，也提出要统筹安全与发展。今年以来密集出台了《数据安全法》《关基保护条例》《个人信息保护法》《网络安全审查办法》(修订草案征求意见稿) 等法律法规、政策制度和监管手段，这些法规和手段都是超前的，强调的是治理先行。

从先发展后治理、同步发展和治理到先治理后发展，从信息化视角看，网络安全出行巨大转折，因此我想说，网络安全迎来了发展新拐点。

在这个新拐点上，首先我们必须转换视角，从业务保障看信息化，从信息化保障看安全，最终实现业务保障视角来看网络安全；其次要转换理念，坚持治理先行，为业务高质量发展营造健康环境；最后我们还要转换发展模式，用系统化和工程化的思想来发展以能力为导向的、信息化跟网络安全深度融合的建设模式。

第二部分：新拐点上的实践和感受

面对新拐点的网络安全变化，奇安信在过去几年做了一些自己的探索和实践。

2019 年，在“十三五”规划中期调整一些重大规划项目实践基础上，我们提出了“内生安全”理念，将安全和信息化深度融合，通过技术融合、数据融合、人员融合，实现网络安全能力与信息化环境融合内生。

2020 年奇安信推出了内生安全框架，把安全方法论与 IT 对标，借鉴信息化的 EA 思想，用系统工程的方法将安全从过去零散的、局部整改为主的外挂式建设模式，走向深度融合的体系化建设模式，构建出动态综合的网络安全防御体系。

基于内生安全框架，2020 年我们帮助很多政企机构完成了“十四五”期间面向数字化保障的网络安全体系规划，实现了网络安全投资在信息化中的占比从 1% ~ 3%，提升到了 5% ~ 10%。

2021 年以来，我们开始跟客户一起，踏踏实实的干活，把规划形成的工程和任务，落地到甲方形成实战化的安全体系。这就是齐总在昨天诠释大会主题时所提出的“经营安全”：实实在在的设计、建设和经营安全体系，保障数字化经营活动安全运转。

在这个过程中，我们遇到了一些问题和挑战，通过创新转变，把问题和挑战变成了机会。

一是新范畴

以数据安全工程为例，数字化的大集成形成了叠加生长，产生了更多的应用与数据。由于数据是流动的，要在云、网、端不同的基础设施中，在不同的业务系统中流转，跟不同的设施和应用形成了缠绕与交织，由此产生了很多安全空白，对安全的覆盖度提出了挑战。

与传统的安全防护不同，构建大数据安全防御体系，不仅要考虑到抵御威胁与攻击的数据实体与计算环境的安全防护，还要将基于零信任架构的动态细粒度访问控制能力与业务应用结合，实现对数据流转的精确控制，做到“主体身份可信、行为操作合规、计算环境与数据实体有效防护”；同样在安全管理层面，除了用于安全攻防的分析、事件响应处置的安全管理中心，也要扩展到进行权限管理、认证管理、审批管理的安全策略中心。

在这个过程中就生长出很多的新安全能力，安全的范畴发生了改变。

二是新管理

随着数字化的深入，信息化和业务深度结合，信息化系统起到了核心业务支撑的作用，信息化成为业务生产资料，性质发生了改变，需要用管理生产资料的方式，融入到企业管理和经营过程，上升到企业更高一级的管理，这种性质的改变，对软件供应链的安全管理提出了挑战。

软件供应链安全，不仅要考虑供应链的自主可控，防止断供、卡脖子的问题，也要将安全与应用开发的生命周期相结合。

因此，我们需要全面梳理、掌握应用系统与供应商的整体情况，通过技术和管理手段排隐患、促能力，整改产品和供应商的现有隐患，建设供应链安全检测能力，然后建机制、抓落实，形成常态化、流程化的供应商安全管理体系，构建更加安全可控的软件供应链安全环境。

软件供应链安全的本质是管理的转变，包括管理理念和管理模式的变化。

三是新模式

以系统安全为例，信息化系统已经融入业务，以服务化方式成为业务的重要支撑，其中 IT 运维是信息化最重要的工作过程之一。以资产为核心，进行配置、漏洞、

补丁整体安全管理的系统安全，是与 IT 运维工作关联最紧密的安全运营工作。

系统安全需要依托大数据架构，获取经过融合的资产信息数据、安全配置信息、漏洞信息数据、补丁数据，在系统安全平台进行数据处理、碰撞和关联，通过指引系统安全的运行过程，通过安全策略管理及漏洞修复等进行系统安全风险的防控。

系统安全工作不仅要落实到大数据平台和自动化工具上，还要把闭环的运行工作落到安全服务工作及 IT 运维服务工作中，全面提升系统的保障能力。

原本小规模、边缘化的安全运营，通过流程、规程、技术、数据的融合最终融入 IT 运维和数字化业务运营的大流程，形成对业务真正有效的保障。

这时候安全的角色就发生了变化，已经融入了 IT 和业务，转变为运营者和保障者。

四是新范式

网络安全从原来的工具产品变成应用系统。以态势感知为例，态势感知是多种安全能力、安全功能集成组合成的复杂系统，是集合了多种工具、设备、平台和人的应用系统，这种复杂性给系统组合和能力集合带来了挑战。

态势感知在我国已经发展多年，目前的态势感知主要分为三种：一种主用于监管机构，我们称之为监管类态势感知；一种主要用于政企机构自身的安全运营，我们称之为运营类态势感知；还有一种主要用于实战演练，我们称之为攻防类态势感知。在这个过程中，奇安信也一度发现态势感知的发展，总是很难完全跟上不同类型客户的变化需求。

我们意识到，态势感知不再是一种独立的安全工具，其本身也需要符合大数据平台与应用的标准，去构建基于元数据驱动的数据平台、数据服务与安全应用。解决数据接入、处理、数据组织、数据治理、数据服务、模型资源、业务应用组件等问题。这样一来，态势感知的构建，也成为了一个复杂的数据平台与应用系统的构建过程。

从原来的工具、设备转变成为平台系统，这就带来了安全范式的转变。

无论是范畴的转变、管理模式的转变、运行模式的转变，还是安全范式的转变，都是在新拐点上，安全与信息化深度融合过程中，我们必须要面对的挑战和机会。

第三部分：新角色、新能力、新生态

在数字化时代的网络安全新征程上，网络安全从业者要主动转换新角色、发展新能力、共建新生态。

第一，我们需要从旁观者转变为共同建设者。

在建设过程中，安全从业者要从一个旁观者、一个滞后的配套工作者转换为积极的共同建设者，因为数字化时代，安全是前提而不再滞后，与信息化是一体两翼，以内生的方式，通过同步规划、同步建设和同步运营，全程参与到数字化建设中。在运营过程中，安全从业者要把安全从审计、检查、整改的检查者转变为运营职能的主动承担者，融入网络和 IT 运营流程，成为数字化业

务运营大流程的一部分。

这个转变就是我们要从有限责任成为无限责任承担者：随着信息化对业务的重要性越来越高，安全的重要性也越来越高，安全深度参与到了信息化和业务发展和运营中，需要真正承担起确保业务安全的无限责任。

第二，在强化非功能性能力的基础上，拓展功能性新能力。

威胁导向的安全能力，比如，态势感知、威胁情报、威胁监测等对于信息化系统是非功能性，技术上自成体系，脱离于信息化之外，但对于应对威胁不可或缺，需要伴随着威胁的不断升级持续强化。

除了强化非功能能力，更重要的是要拓展原本缺失的安全能力，融入业务和应用，成为功能性能力。比如，攻击面管理、沙箱、UBA 这些原本外挂的能力，随着积极防御的演进，开始进入信息化和业务循环，成为功能性能力。

在建设层面通过安全左移的 DevSecOps，进入应用从开发到应用的全流程；在运营层面把流程、技术、数据融入 IT 和业务运营的大流程，融入数字化的业务运营，都是将安全拓展成为数字化业务功能性能力的举措。

通过功能性能力的发展，原本业务和信息化对安全的恐惧就会慢慢降下来，安全反作用于信息化和业务的变革，由障碍变成为推力，真正成为数字化生产力。

第三，产业链中的各环节需要融合发展，共同构建新安全生态。

之前的安全生态是安全厂商的生态，更像是我们圈子内的事情。在现在的数字化时代，安全生态亟需破圈，打破小圈子。在甲方的安全生态中，不仅有安全处、安

全口的人和组织，还需要加入信息化处、数据办、业务部门，甚至和企业管理层建立起覆盖数字化业务全流程的、各层级的真正的数字化安全生态。

在乙方的安全生态中，不仅有安全厂商，还必须把大的集成商、平台厂商、科技厂商、信息化服务提供集成商结合在一起，构成包含数字化建设全过程、各环节的一个新的数字化安全生态，推动数字化时代的安全，承担起数字化使能者的使命，让安全成为数字化生产力，成就美好的数字化未来。

随着法律法规密集出台，今天的网络安全市场一片欣欣向荣，但是作为一个从业者，我也有很多担忧，这么多的法律法规，每一个都自成一个体系，有自己的范畴、有各种要求，而且要求越来越高，但是作为任何一个企业，在数字化过程中，正处在 IT 与业务变革的探索中，可能没有太多的精力去逐一实现所有体系的每个条款，只能集中力量办大事。

我们提出的内生安全框架就是通过工程化的方法，通过十大工程和五大任务来满足各种需求，帮助客户搞好建设、做好运营，满足各种法律法规要求。所以希望我们大家在一起，基于内生安全框架，脚踏实地推动每个工程的落地，满足每一条法律法规的要求，真正助力国家和政企“十四五”的数字化转型，这就是我们在新拐点上的新征程。安

规划一步快一步

奇安信

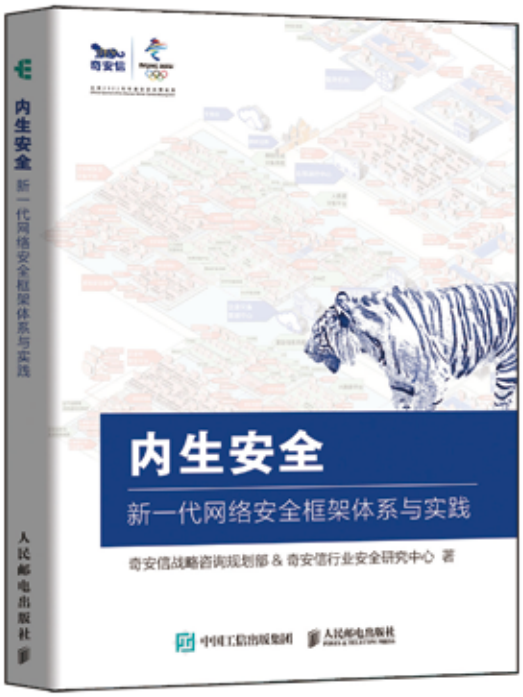
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

澎湃 THE PAPER
2021 年 08 月 27 日

BCS 2021 产业峰会：网络安全产业迎来新拐点

数字技术日新月异，网络安全已成智能社会新基座。近期，全球行业法规、政策密集出台，推动治理先行，网络安全产业正迎来新拐点。8 月 27 日，北京网络安全大会（BCS 2021）产业峰会线上启幕，来自全球多个国家和地区的网络安全行业专家展开对话。与会专家指出，要保障信息化系统与安全体系深度融合，应转变网络安全保障思维，实现治理先行、同步发展。

产业峰会与战略峰会、技术峰会并称 BCS 2021 三大峰会，是全球网络安全业界专家年度对话的平台。峰会上，国家创新与发展战略研究会副会长、北京网络安全大会顾问委员会主任郝叶力，全球权威的 IT 研究与顾问咨询公司 Gartner 杰出研究副总裁、头牌分析师尼尔·麦当劳（Neil MacDonald），中国电子信息产业集团有限公司党组成员、副总经理陈锡明，世界卫生组织首席信息安全官弗拉维奥·阿焦（Flavio Aggio），中国联合网络通信集团有限公司副总经理梁宝俊，腾讯云计算（北京）有限责任公司副总裁马斌，百度安全手机科学家李康，奇安信总裁吴云坤等发表了主旨演讲。美国洛杉矶市首席信息安全官蒂莫西·李（Timothy Lee）、美国全国大学体育协会的首席信息安全官威廉姆·贾德（Judd William）、思科首席信息安全官顾问团队负责人温迪·纳瑟（Wendy Nather）等展开全球 CISO 对话，围绕首席信息安全官这一职务的理解、信息安全产业的

国家创新与发展战略研究会副会长、北京网络安全大会顾问委员会主任郝叶力

未来等展开分享。

新变量：网络安全产业迎来拐点

“安全应变而动！”郝叶力首先亮明观点，“数字时代，安全正在发生重大变革。”

郝叶力认为，新变量表现在四个方面。首先，新技术快速激变带来新挑战。云计算、大数据、人工智能、区块链等新技术帮助用户利用海量数据，并从中获取巨大价值，但同时带来了巨大的威胁和风险，拓展了网络安全的应用领域。

其次，新基建带来新要求。“十四五”规划要求围绕数字转型、智能升级、融合创新布局基础设施，融合基础设施和创新基础设施释放了新动能，但也对网络安全系统提出了更高要求。

三是数字化转型带来新任务。2020 年 8 月 21 日，国务院、国资委印发了《关于加快推进国有企业数字化转型工作的通知》，产业互联网和产业数字化将成为国家的着力点，网络安全行业接到了新任务。

四是政策导向带来新标准。强监管，牵动了安全产业升级。随着国家网络空间安全战略、《网络安全法》《数据安全法》《网络安全审查办法》《网络安全等级保护 2.0 制度》《关键信息基础设施保护条例》相继出台，从制度、管理、系统防护、供应链上下游数据流动等方面，形成了安全行为准则的完整政策导向。

“如何抓住这些新变量，用好新机遇，需要我们打开新视角，开拓新思维。” 郝叶力说。

尼尔 · 麦当劳则从全球网络安全局势进行研判：“我们所有人都面临着持续的安全挑战。造成安全挑战的因素包括疫情导致线上办公的增加，世界范围内对于隐私

中国电子信息产业集团党组成员、副总经理陈锡明

权法规的强化，现代应用程序架构（包括 Kubernetes 中的容器）复杂性和规模的增加，我们需要支持的移动设备和不受管理的设备等端点的多样化，以及攻击技术

奇安信集团总裁吴云坤

的不断升级等。”

“网络安全迎来了发展新拐点。”站在行业视角，网络安全产业的时代变革性特征更为突出。吴云坤从信息化的视角回顾了过去 25 年网络安全发展历程后发现，信息化与网络安全经历了从先发展后治理、同步发展和治理、到治理先行的历程，这种转折表明网络安全行业迎来新拐点。

“在这个新拐点上，我们必须转换视角，要从信息化和业务视角看安全，要转换理念，坚持治理先行，为业务高质量发展营造健康环境。同时，应该用系统化和工程化的思维来构建安全系统，实现信息化和网络安全深度融合。”吴云坤说。

新技术：协同保障网络安全与产业发展

站在新拐点上，哪些技术能够更有效地做好网络安全保障呢？行业专家们贡献了各自的解决方案。

奇安信在 2019 年提出内生安全理念，2020 年又推出内生安全框架。吴云坤说，内生安全框架正在发挥越来越大的作用。2020 年奇安信帮助很多的政企机构完成了“十四五”期间面向数字化保障的网络安全体系规划，实现了网络安全投资在信息化中的占比从 1%~3%，提升到了 5%~10%。

伴随着实践的丰富与深化，内生安全框架在各类攻防实践中也得到丰富与拓展。吴云坤总结出“四新”，即新范畴、新管理、新模式、新范式。具体来说，在数据安全等一些新场景中，需要不断生长出新能力填补空白，安全范畴发现变化；信息化成为业务生产资料，需要用管理生产资料的方式，融入到企业管理和经营过程，管理模式发生变化；安全运营从原本小规模、边缘化的安全运营，开始融入 IT 运维和数字化业务运营的大流程，这是运行模式的变化；安全原来的工具产品变成平台和应用系统，安全范式发生变化。

陈锡明在峰会上推介了 PKS 安全体系，他说，这是一种以内生安全为核心特征的数字化业务支撑体系，

以可信计算、内存保护、指令流安全预检测三大安全技术为根基，实现“防断供、关后门、堵漏洞”等核心自主安全能力，是一种安全、先进、绿色的通用计算体系。

梁宝俊则透露了中国联通在 5G 时代的全新布局。他说，近年来，联通布局形成了 5G+ABCDE 的能力，在 5G 网络、千兆光宽、云化等基础上，构建了人工智能、区块链、联通云、大数据、边缘云为核心的创新能力的整合体系，囊括了以云原生为核心，具有安全可信特点的联通云，可信的联通链及大数据安全能力等。这一技术目前正在全国多地落地发展。

马斌和李康也分别介绍了腾讯在云安全领域、百度在 AI 安全领域的最新技术进展及其效果，展现出相关领域最前沿的网络安全动态。

中国联合网络通信集团有限公司副总经理梁宝俊

新生态：融入数字化运营大流程

“在数字化时代的网络安全新征程上，网络安全从业者要主动转换新角色、发展新能力、共建新生态。”吴云坤在峰会上呼吁。在吴云坤看来，网络安全从业者需要从旁观者转变为共同建设者，融入信息化和业务流程，成为数字化业务运营大流程的一部分。

重视网络安全中人的因素，也是世界卫生组织首席信息安全官弗拉维奥 · 阿焦的关注点。新冠疫情发生后，世界卫生组织的网络安全也面临着挑战，弗拉维奥 · 阿焦说，除了在技术上做好防御，根据当前网络安全形势，他正在教会员工和承包商如何在家更安全地上网。“仅靠技术远远不够。人为因素起着重要作用。当然，包括培训、定期网络钓鱼演习、简报在内的网络安全计划也非常重要。”

吴云坤说，“除了在人的层面做出改变，网络安全行业在能力发展和生态建设方面也要做出改变，一是在强化非功能性能力的同时，拓展功能性新能力；二是在产业链中的各环节需要融合发展，共同构建新安全生态。最终更好地保障网络安全。”

“希望我们大家在一起，基于内生安全框架，脚踏实地推动每个工程的落地，满足每一条法律法规的要求，真正助力国家和政企‘十四五’的数字化转型，这就是我们在新拐点上的新征程。”吴云坤说。安

中国青年报 CYOL.COM

构建网络空间法治基石，营造良好数字法治生态

2021 年 8 月 26 日下午，首届“中国网络与数据安全法治 50 人论坛”亮相北京网络安全大会 (BCS 2021)。本届论坛作为北京网络安全大会 (BCS 2021) 系列重要论坛之一，以“构建网络空间法治基石 营造良好数字法治生态”为主题展开。

本届论坛由中国行为法学会和中国通信学会指导，网络空间治理与数字经济法治 (长三角) 研究基地、中国通信学会网络空间安全战略与法律委员会、中国政法大学数据法治研究院、中国数字经济安全与发展 50 人论坛、华东政法大学数字法治研究院、浙江大学国际战略与法律研究院、中国电信研究院安全工程中心、奇安信集团联合主办。

中国政法大学副校长、数据法治研究院院长、中国通信学会网络空间安全战略与法律委员会主任委员时建中教授表示，在数字化时代，身份、行为乃至社会关系都已经数据化、数字化，数据治理是一个必须正视的问题。无论是为了维护安全或者促进发展，数据行为的监管都显得格外重要。而且，数据监管涉及到社会治理、经济发展和政府管理等各个领域、各个方面、各个环节。因此，我们需要尽快建立数据协同监管的协调机制，同时加快电信法的制定工作，来推动基础电信业务的发展，维护基础电信设施和业务的安全。

中国行为法学会副会长、天津大学法学院院长孙佑海教授表示，强化数据安全法治是维护国家安全的迫切需要。数据是国家基础性战略资源，没有数据安全就没有国家安全。我们应该积极贯彻《数据安全法》，通过促进数据依法合理有效利用，充分发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济，更好地服务我国经济社会的创新发展和可持续发展。

中国法学会航空法学研究会会长、中国东方航空集团公司总法律顾问郭俊秀围绕“《数据安全法》和《个人信息保护法》驱动企业数据合规行稳致远”主题发表演讲，他表示《数据安全法》和《个人信息保护法》为依法规范处理数据活动提供了基本遵循，应依据国家相关规定履行网络安全等级保护和数据分类分级的法律义务，结合地区、行业、领域建立重要数据的保护制度，在企业内部明确指定数据安全工作负责人和归口管理部门，重点关注自动化决策、利用数据实施不正当竞争等领域的数据安全和个人信息保护问题。

浙江大学教授、浙大宁波理工学院启新讲座教授、网络空间治理与数字经济法治 (长三角) 研究基地主任兼首席专家、联合国世界丝路论坛数字经济研究院院长、中国通信学会网络空间安全战略与法律委员会副主任王春晖认为，数字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，构建良好的数字生态应当让数字社会的“五维空间”更智慧、更便捷、更效率、更安全。网络安全法、数据安全法和个人信息保护法是构建良好数字社会生态的三大基石，维护关键信息基础设施安全是网络安全的基石 ; 统筹数据发展与安

全是数据安全的基石；规范个人信息处理活动，保护个人敏感信息是个人信息保护的基石。

中国移动通信集团有限公司法律与监管事务部总经理于莽发表了题为《携手共建 5G 时代的数据安全治理体系》的演讲，于莽建议尽快出台相关的配套法律法规，对数据活动的各参与主体权利、义务和责任等进行细化，明确分类分级标准、具体重要数据目录、监管流程等内容；同时，要积极开展有关数据安全行业标准、数据领域法律问题研究等社会活动，充分发挥“法律也是竞争力、政策也是生产力”的作用，为助力数字经济高质量发展提供坚实法治保障。

华东政法大学数字法治研究院院长马长山以“网络空间安全法律法规体系化建设剖析”为题发表演讲，他认为应严格落实《网络安全法》及其配套规定，积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

浙江大学教授、国家社会科学基金重大项目“建立健全我国网络综合治理体系研究”首席专家、浙江大学国际战略与法律研究院常务副院长程乐，以“从勒索软件看网络空间国际治理”为题，重点研判了数据安全的国际化治理问题。程乐认为，随着勒索病毒的日益猖獗，国家应提高关键领域、特定人物的网络防范水平和意识，同时加大研发投入，构建多层防御体系立法先行，推进全产业链常态化治理，推进反勒索软件商业化，从而完善法律保障，为网络空间治理保驾护航，同时也要加强国际合作，建立信息、技术共享机制。

围绕网络爬虫合法边界问题，全国律协网络与高新技术委员会副主任、北京市律师协会科技与大数据委员会主任陈际红认为，公司应严格遵守《数据安全法》第三十二条的规定，收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。通过爬虫收集、处理个人信息的，应当遵循《个人信息保护法》第二十七条的要求，即可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

关于数据跨境流动的合规与风险，中国通信学会网络空间战略与法律委员会委员、德衡律师集团数字经济

和人工智能业务中心总监辛小天表示，应积极推动数据出境标准的落地和“同意”规则的适用，同时加速制定去标识化等技术标准，并增强对域外法律理解和适用，从而提升中国“朋友圈”和国外政府对中国法律环境的评价。

奇安信数据安全研究院副院长、奇安信首席数据安全架构师韩培义以“数据生产要素时代的关基安全保障技术与实践”为题，重点探讨了数据生产要素时代的数据安全责任与实践。韩培义表示，随着国务院将数据作为一种新型生产要素写入政策文件，企业应设立跨部门数据管理组织机构，进行跨部门数据使用与安全策略制定，同时开展数据安全治理和数据安全保护体系建设，并针对数据访问与使用、数据共享交换、数据交易等，制定不同的安全措施，从而全面提升数据安全能力。

主旨演讲结束后，王春晖教授主持了圆桌对话，对话围绕“《数据安全法》和《个人信息保护法》下的企业数据合规”展开对话，工业和信息化部信息通信经济专家委员会委员、北京浩瀚深度公司董事长张跃，北京师范大学网络法治国际中心执行主任吴沈括，网络空间治理与数字经济法治（长三角）研究基地研究员、浙大宁波理工学院副教授卢剑峰，南京领行科技股份有限公司（T3 出行）CEO 崔大勇，中国电信研究院安全工程中心资深专家秦达，中国通信学会网络空间安全战略与法律委员会副主任委员、上海市光明律师事务所主任王树平，奇安信集团首席法律顾问马兰参与了圆桌对话。

对话嘉宾一致认为，《数据安全法》和《个人信息保护法》开启了企业数据合规的新篇章，企业应当建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；企业处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围，在履行“告知－同意”规则的基础上，采取对个人权益影响最小的方式和处理目的在最小范围处理个人信息。

“中国网络与数据安全法治 50 人论坛”每年将围绕网络与数据安全法治领域的重大理论和实践问题展开研讨，并不定期地举办网络与数据法治高端研讨会和报告会，积极为国家和地方的网络空间治理与数字经济法治建设提供智力支撑。安

图：第五届网络安全产业担当与发展高峰论坛嘉宾集体合影

網易 NETEASE

2500 亿市场 中国网络安全企业的机与责

8 月 26 日，2021 北京网络安全大会正式开幕。作为大会的重要组成部分，由中国计算机学会计算机安全专业委员会主办、奇安信集团承办的第五届网络安全产业担当与发展高峰论坛成功举行。

近百家网络安全骨干企业代表参与了线上云峰会，围绕“共担安全使命，共创产业未来”主题，深入探讨产业发展机遇背景下的中国网络安全企业的机与责。BCS 大会顾问委员会委员、CCF 计算机安全专业委员会荣誉主任严明主持了本次论坛。

规模将超 2500 亿元，产业进入爆发期

2021 年，我国网络安全产业迎来史上最佳的政策环境，政企客户的安全应用场景进入爆发期。

2021 年 7 月，工业和信息化部公布的《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》提出，到 2023 年，我国网络安全产业规模将超过 2500 亿元，年复合增长率超过 15%。此外，还规定电信等重点行业网络安全投入占信息化投入比例不低于 10%。目前多个地方政府也在规划推动网络安全发展的政策。例如，上海拟在网络安全“十四五”规划中明确，政府和公共企事业单位在网络安全上的投入比例不低于 10%。

与会安全企业高层认为，面对前所未有的政策环境和产业爆发机遇，网络安全行业需要以开放融合的心态，建立更加紧密的合作关系，推动技术创新和产业发展。

CCF 计算机安全专业委员会主任、公安部一所副所长于锐指出，网络安全企业需要树立创新发展、高质量发展的理念，抓住“十四五”数字经济与网络安全融合

发展的契机，在两个一百年的历史交汇期交出网络安全产业担当与发展的满意答卷。

他同时提出，希望我国安全企业家们，抓住当前数字化转型的时代大潮，贯彻落实国家的总体安全观，针对国家网络安全建设的重点、焦点、难点工作持续投入，为营造良好的产业生态环境，做大、做强产业经济，发挥更多作用。

三个方面发力，做好网络安全守护者

针对网络安全的颠覆性变化，奇安信集团董事长、北京网络安全大会主席齐向东认为，网络安全企业应该朝三个方面发力，做好数字时代网络安全的守护者：一是突破 IT 时代粗犷的信任体系，建立动态可控的信任体系；二是破解数字技术新应用场景的安全难题，推动网络安全向实战化发展；三是提供网络安全运营服务水平，帮助客户建立常态化的安全能力。

“用安全可信构筑网络主动免疫保障体系，把安全掌握在自己手中。”中国工程院院士沈昌祥在主题演讲中指出，当前我国已进入可信计算 3.0 时代，完备的可信计算 3.0 产品链，将形成巨大的新型产业空间。按照网络安全法、密码法、等级保护制度、关键信息基础设施保护制度的要求，全程治理，确保体系结构、资源配置、操作行为、数据存储、策略管理可信，以开创网络空间安全主动免疫新生态。

针对网络安全新生态建设，绿盟科技首席解决方案专家刘弘利介绍了具有“全场景、可信任、实战化”安全运营能力的智慧安全 3.0 安全理念。安芯网盾 CEO 姜向前则从技术角度分享了内存安全保护对于强化安全防御体系的重要作用。

构建可信网络环境基石

为了更好建立动态可控信任体系的基础，由奇安信可信浏览器、银河麒麟操作系统、统信操作系统联合发起的“商用密码证书可信计划”在论坛上正式发布，该计划将公开接受国密数字证书发布机构入根申请，并为所有国密开发者免费提供各平台的奇安信可信浏览器国密开发者专版，为国密从业者提供便利，以协助国密证书技术持续升级，协助建立中国的证书可信审计机构，促进行业的开放合作及蓬勃发展。

数字认证、上海 CA、广东 CA、深圳 CA、亚洲诚信等十四家主流 CA 机构在线上见证了发布仪式。

数字认证总经理林雪焰表示，“数字信任的驱动，将有助于提升各行业的价值潜力。” 在现实世界及网络空间之间，通过身份可信、行为可信、数据可信的密码服务，将为用户搭建安全信任的桥梁，也将在保护用户数据安全和隐私，保障业务运行的法律合规性等方面带来极大便利。

作为“商用密码证书可信计划”的联合发起单位，统信软件高级副总经理、CTO 张磊，麒麟软件副总裁、安全研发总经理杨诏钧，分别介绍了统信 UOS 创新生态体系和麒麟系统持续创新的自主安全体系。作为国产操作系统的代表厂商，信创企业的积极创新对于产业生态持续健全也将产生巨大作用。

据悉，“商用密码证书可信计划”未来还将联合全国数十家 CA 机构，共同为国产密码证书的推广应用，继续创新合作模式，共同探索协同路径，为完善国产密码信任体系添砖加瓦，贡献力量。

圆桌对话环节，在中国信息安全原副社长、主编崔光耀主持下，来自奇安信、安恒信息、安博通、山石网科、格尔软件、华为云、麒麟软件、江南信安、江南天安的 9 位嘉宾，围绕“十四五”时期，各企业如何充分发挥企业责任感、参与行业生态建设，展开了积极讨论。

其中，奇安信集团副总裁陈华平重点分享了关于构建产业生态的观点。以此次宣布的“商用密码证书可信计划”为例，他表示，浏览器和操作系统，是底层的支撑和入口级的产品。商业密码证书和浏览器厂商、操作系统厂商，在信创领域做好预装和适配，将对整个密码产业产生促进和推动作用。而整个产业生态，也需要每个企业各司其职，共同努力，来推动产业的发展、壮大和繁荣。安

证券日报 SECURITIES DAILY

探真科技荣膺总冠军 新场景安全受热捧

8 月 27 日，由奇安信科技集团股份有限公司、全国网络信息安全创业投资服务联盟（筹）、北京房山区金融安全产业园、奇安（北京）投资管理有限公司联合主办的 2021 安全创客汇总决赛圆满落幕。

在经历了初赛、明星赛、决赛等多个环节评选，以及前五届安全创客汇冠军企业的“终极面试”，北京探真科技有限公司脱颖而出，问鼎第六届安全创客汇十强总冠军，并获得奇安投资的 2000 万投资意向。

“关保元年”已至 网络安全行业迎来更多机会

8 月 17 日，国务院颁发《关键信息基础设施安全保护条例》，为我国深入开展关键信息基础设施安全保护工作提供有力法治保障，也为我国深入开展关键信息基础设施安全保护工作提供有力法治保障。

“关保元年已经来到，给企业带来了更多要求，也给网络安全行业带来了更多机会。”奇安信集团董事长、北京网络安全大会主席齐向东在致辞时表示，网络安全和漏洞的斗争，不只是系统中的漏洞，操作过程、管理要求、规范制度、工作流程等环节中的漏洞或薄弱环节，都是潜在的网络安全威胁。只要网络威胁没有被彻底消灭，安全行业就会不断发展。

而网络安全要想实现质的飞跃，离不开资本的力量。一方面，网络安全行业的“体系化”建设亟待资本入场；另一方面，网络安全企业的技术创新、服务创新需要资本赋能。“奇安信在上市前，获得了资本的投入，用于网络安全科技创新领域。希望通过搭建安全创客汇这一平台，为网络安全营造健康和谐的创投生态添砖加瓦。”

据统计，安全创客汇从 2016 年开始举办，进入总决赛的 50 家企业在赛后，有 90% 获得了融资，总融资额超过 25 亿元。而今年也邀请到了元禾重元基金、中信建投、国投创合、IDG 资本、诚通基金、国新风险投资、银河创新资本、中国电信、沸点资本、云晖资本、中科创星、中电智慧投资投资、天风天睿、国开开元、晟龙元和、嘉豪投资、百度风投、密码资本、天创资本、启迪科服、元起资本、领泓资本、常垒资本等多家相关创投资本及相关机构参与。

赛制创新 全面发掘明星企业潜力

为了充分发掘明星企业的优势和特长，安全创客汇在决赛赛制上进行了大胆创新：邀请前五届安全创客汇冠军企业代表齐聚赛场，选一位冠军候选人进行互动提问，来了一场“终极大考”，评委参考问答表现进行最终评分。

芯盾时代、众享比特、永安在线（原威胁猎人）、全知科技、安芯网盾 5 家企业，通过安全创客汇平台，获得更大的发展空间和资源支持，也收获了更好的成长。面对仍在初创阶段的企业，这些企业代表也从技术实力、人才激励、发展规划等方面，更有针对性的提出问题，以期帮助候选企业充分展示自身实力和优势。

根据候选企业在问答中的表现，在奇安信集团总裁、安全创客汇评委会主席吴云坤，北京赛博英杰科技有限公司董事长、安全创客汇评委会副主席谭晓生，奇安信集团副总裁、安全创客汇评委会主任陈华平，奇安投资 CEO、安全创客汇评委会副主任王鹏飞，国投创合总经理刘伟，金融安全产业园常务副总经理高赫和投资机构代表、网络安全产业专家、研究机构的专家代表的严格评审下，2021 安全创客汇冠军新鲜出炉。

北京探真科技有限公司、北京安帝科技有限公司、北京未来智安科技有限公司、北京擎天信安科技有限公司、北京数安行科技有限公司、上海富数科技有限公司、上海碳泽信息科技有限公司、北京天防安全科技有限公司、上海物盾信息科技有限公司、苏州至赛信息科技有限公司跻身 2021 安全创客汇十强。

作为聚焦网络安全领域的专业创投平台，有越来越多的安全行业初创企业，将安全创客汇视为寻求行业认可和获取资本助力的最佳平台。而安全创客汇组委会也通过不断创新升级，成长为涵盖创客明星赛、创客沙龙、创业培训等多主题、多活动、多服务的创新生态平台。未来，安全创客汇也将持续为优质资本和创新企业搭建交流平台，持续推动安全产业的创新发展。安

人民邮电

护航数字经济发展，开拓产融安全机遇

2021 年 8 月 27 日，由中国信息通信研究院和奇安信集团共同主办的“2021 北京网络安全大会通信行业网络安全论坛”成功举行。论坛以“护航数字经济发展，开拓产融安全机遇”为主题，围绕通信行业建立常态化与实战化的安全运营体系，在产业融合等数字化转型场景中创新服务模式，保障软件供应链安全等话题展开。

工业和信息化部网络安全管理局网络与数据安全处副处长袁春阳、奇安信集团总裁吴云坤为论坛致辞。中国信息通信研究院副院长魏亮、中国电信集团网络和信息安全管理部副总经理张侃、中国移动集团信息安全管理与运行中心副总经理袁捷、中国联通集团数字化部 (信息安全部) 副总经理谢攀、奇安信集团代码安全事业部总经理黄永刚、中兴通讯股份有限公司副总裁王继刚、CableLabs 移动网络安全公司首席架构师万涛发表主题演讲。论坛主持人由中国信息通信研究院安全研究所副所长 (主持工作) 谢玮担任。

袁春阳副处长在致辞中指出，通信行业基础电信网络、重要互联网基础设施等对于全行业具有基础支撑作用，保障通信行业网络安全工作要从落实企业主体责任、强化技术能力建设、做好安全服务支撑、发挥行业自律作用等方面入手，不断完善通信行业网络安全防护体系。

随后，奇安信集团总裁吴云坤通过视频为论坛致辞。吴总介绍了网络安全与通信行业协作的重要性，并结合奇安信的实践探索提出如下建议：第一，共同发展面向数字化场景下的新安全能力，如数据安全、应用安全等领域的能力。第二，共同探索集约化的安全基础设施建设和集约化服务新模式。第三，共同建设全面融合、深度协同的安全产业生态。

论坛上，魏亮副院长与张侃副总经理、袁捷副总经理、谢攀副总经理、叶臻院长、奇安信集团曲晓东高级副总裁等筹建单位领导共同发布“通信行业软件供应链安全社区”。通信行业软件供应链安全社区将致力于行业软件供给过程的安全生态建设，围绕落实国家法律法规和行业主管机构要求，通过将运营商、供应商、安全厂商及专业评测机构联系起来形成生态圈，推动探索软件供应链安全标准、协同管理流程、划分风险责任、孵化创新技术，促进软件供应链安全生态良性循环。

在主题演讲环节，魏亮副院长围绕“通信行业软件供应链安全治理”分享了他的观点，并提出四点建议。一是防护关注点由“运行阶段”向“全生命周期”转变，二是治理模式由“自治或半自治”向“共治”转变，三是构建可信体系，寻求敏捷开发与安全成本平衡新切入点，四是供应链安全治理工作由“被动式”向“引领式”转变。

张侃副总经理就“安全融云，打造网信安全能力底座”作主题报告，他提到，安全融云是夯实企业高质量发展的底座。在安全融云的探索实践中，中国电信展开了五项计划，包括通过技术、管理、运营，三管齐下，打造安全的云基础设施；建立 1+31+N 的数字化安全中台；以“三化”为基础搭建安全能力池；打造覆盖移动安全、Web 安全、数据安全、物联网安全等多领域的系列安全产品和服务；推动战略合作，联合构建网络安全生态。

袁捷副总经理以“5G 扬帆，安全护航”为主题发表演讲，他表示，中国移动已实现在重点 5G 垂直行业的安全能力覆盖，在全国范围内面向 5G 重点赋能领域开展“安全样板”建设，打造了一批如 5G+ 智能电网、5G+ 智慧港口、5G+ 车联网、5G+ 智慧工厂、5G+ 智慧矿山的安全样板间。

谢攀副总经理结合中国联通集团的实践经验，围绕“中国联通常态化安全运营探索实践”作主题报告，介绍了“横向到边，纵向到底”的网络与信息安全体系架构。中国联通充分践行安全运营“常态化”原则，构建安全调度指挥体系，在终端安全、数据安全、信安专项等领域取得了积极成效。打造数字化敏捷底座，为 5G 融合创新应用和工业互联网等新业务场景的安全运营奠定了坚实的基础。

黄永刚总经理以“软件供应链安全实践”为主题，分享了多个奇安信在软件供应链安全方面的相关实践，他表示，供应链安全要打“团体赛”，需要监管机构、最终用户、软件厂商等主体携手共进，建立软件供应链安全风险的发现能力、分析能力、处置能力、防护能力。

王继刚副总裁发表题为《企业数字化转型安全方案》的主题报告，他表示，企业数字化转型在安全方面要做到两点目标，即防入侵和防泄密。基于数据流动、无边界访问、业务上云、安全运营、产品安全交付五类数字化转型的典型场景，王总分享了中兴通讯安全防护的主要思路。

万涛首席架构师以线上的形式发表题为《通信网络的架构和安全风险演变》的主题报告，他认为，4G 安全的攻击主要针对终端用户，少数攻击针对核心网；而 5G 核心网的攻击面呈多样化、复杂化，运营商和各大企业应把未来的重点聚焦于核心网的安全防护。

本次论坛，与会嘉宾围绕论坛主题展开深入交流，探讨数字经济发展中的安全问题与解决方案，并呼吁行业各界同发展共创造，形成网络安全发展合力，推动网络安全能力再提升，为数字中国建设贡献行业力量。安

金融界 JRJ.com

内生安全 引领金融新基建

8 月 27 日，由中国金融电子化公司主办，奇安信集团、中电金信软件有限公司共同承办的，主题为“内生安全 引领金融新基建”的 BCS 2021 金融网络安全论坛在京顺利召开。中国金融学会金融科技专业委员会秘书长兼副主任委员杨竑，中国电子信息产业集团有限公司党组成员、副总经理陈锡明，中国金融电子化公司副总经理潘润红出席会议并发表了致辞。

会上，三位致辞嘉宾与中国工程院院士郑纬民、金融信息化研究所 (FITI) 副所长习辉、奇安信集团副总裁张翀斌共同发布了 FITI 金融信息安全成熟度模型。该模型参考相关的标准、规范、要求、研究成果，并结合我国金融业网络安全现状，打造出适合金融行业特性、可量化可评估的网络安全能力成熟度模型，为金融机构自评估提供指导，也为监管机构指导工作提供依据，有助于统一金融业网络安全评估标准，提升行业整体网络安全能力水平。

金融信息化研究所贺冠华博士对 FITI 金融信息安全成熟度模型的背景、内涵、参考依据、应用价值等做了深入解读。贺冠华表示，金融业网络安全和信息化“十四五”发展规划明确提出了研制网络安全能力成熟度模型的要求。金融信息化研究所兼顾规范性、可用性、体系性和可操作性的原则，通过安全能力、安全域和能力成熟度等级三个维度重点打造满足合规要求的、可量化、可操作的成熟度模型，帮助金融机构评估自身网络安全水平，

图：多位院士专家代表共同发布 FITI 金融信息安全成熟度模型

确立网络安全建设目标，促进金融行业提升网络安全整体能力水平。

中国工程院院士沈昌祥分享了题为《开创安全可信数字经济新生态》的演讲。他认为，新基建将加速推动我国数字化转型、网络化重构、智能化提升、产业化升级。但是新基建下万物互联网络攻击将从数字空间延伸到物理空间，对网络安全提出严峻挑战，必须有效应对垄断网络空间霸权威慑，筑牢网络安全防线。构建网络安全主动免疫保障体系，落实等级保护要求，保障数字经济健康发展。

中国工程院院士郑纬民发表了《破解金融科技面临的“卡脖子”局面——从头研发先进的系统软件》主题演讲。他表示，金融竞争是当今国际经济竞争的核心，金融新基建将成为夯实金融业竞争优势的重要底座，解决金融科技“卡脖子”问题势在必行，破局方法在于从头研发先进的系统软件。郑院士称，当前新型存储器件、新型程序语言等的出现，为重新设计系统软件带来了机会。他呼吁从头构建先进的系统软件没有想象的那么难，关键是开始做。

中国人民银行金融信息中心信息安全部主任袁慧萍带来了《数字经济时代的数据安全之道》主题分享。她从数据安全法规、数据安全金融行业标准、数据安全实践三个层面做了综述讲解，阐释数字经济时代的数据安全之道。她表示，我国数据安全相关法规体系日趋完善，

落实数据安全责任已经刻不容缓。今年将成为数据安全元年，技术变革、法规遵循、安全攻击事件、要素流通四方面将驱动企业真正重视起数据安全建设。

中国电子信息产业集团有限公司总工程师周进军发表题为《以内生安全应对金融安全挑战》的演讲。他表示，网络安全已进入国家网络时代，传统的打补丁式的安全防护手段已经不能满足需求，需要建立“内生”安全防御体系。“飞腾 CPU+ 麒麟 OS”体系的国产化软 / 硬件平台，以内生安全为思想，以可信计算为根基，实现了动态立体的整体安全防护能力。

中国工商银行安全攻防实验室副主任叶红带来了《商业银行安全测试实践》的主题演讲。她提出，随着敏捷开发要求安全测试时间不断进行压缩、新技术引用带来的新风险、供应链引入的新风险等问题并存，安全测试覆盖率和测试深度给广大金融机构带来了很大的挑战。而通过交互式安全测试技术、移动插桩技术、安卓定制沙盒技术能够有效应对银行安全测试所面临的业务逻辑复杂、移动端攻击下沉、移动端供应链合规风险等问题，同时人工智能对抗也是互联网金融安全测试面临的新挑战。

中国建设银行信息安全管理处处长陈德锋发表了《金融网络安全运营建设实践》报告，主要介绍了建设银行安全运营的实践和展望。他表示，建设银行以信息安全制度策略为指导，围绕信息资产分级分类，对数据及支撑数据的应用、基础设施和物理环境，提供统一完备的安全服务和全生命周期的信息安全管理，通过持续的安全运营，保障客户信息和资金安全，支持业务持续运营。

中国农业银行科技与产品管理局信息安全与风险管理处副处长董金程发表了《金融企业网络安全运营实践及思考》的主题分享。他表示，通过资产目录化、网络安全体系布防、漏洞治理、安全事件的监控和处置、应用研发安全管理体系、红蓝对抗体系等多个专项的推进，农业银行实现了从安全“运维”到安全“运营”的进阶，团队也更注重安全能力与企业业务目标的匹配和融合，强调服务、赋能和价值输出。

平安银行安全架构师何琰带来《从资产视角出发，回归安全风险本质》的主题演讲，分享了大数据在银行安全风险动态管理中实践和探索。她认为，银行安全工作的核心关键在于需要关注核心资产，量化管理过程当中的事前、事中、事后的风险，持续推动其在可控范围内。通过围绕资产和其对应属性，结合标签、画像、风险监测评分指标等工具对风险进行动态评价和跟踪，聚焦重点的风险资产和风险领域，持续推动有针对性的风险管控措施落地，从而站在更高的视角来观测和管理风险。

主管机构高度重视供应链安全，该如何应对？太平洋保险集团信息安全部负责人李丽红做了《软件供应链安全实践与展望》主题演讲，针对供应链安全管理提出了三点建议：一是要立标准，针对国家关键信息基础设施，建立供应链风险管理的行业规范；二是要排隐患，针对金融、电信、能源等关键信息基础设施行业，开展供应链安全专项排查工作；三是要查源头，在软件开发过程中，必须保障源代码安全和供应链安全。

此外，论坛上还举行了圆桌会议，人民银行《金融电子化》杂志社副总编邵山、工商银行数据中心金融科技专家顾骏、交通银行金融科技部安全处处长刘占明、中国银联信息总中心高级总监周恒磊、上海银行信息技术部内控安全部高级经理许思中、北京航空航天大学网络空间安全学院院长刘建伟、北京国家金融科技认证中心首席专家李振等多位嘉宾参与，就安全管理体系、团队建设和人才培养等话题进行了深入探讨。

作为 2021 北京网络安全大会重要议程之一，金融网络安全论坛以主题演讲与圆桌会议结合的形式，邀请了金融行业机构代表、信息化专家、网络安全专家等齐聚一堂，聚焦金融数字化转型和金融新基建、国家法律法规和行业监管要求、网络安全风险，分享和探讨了先进金融机构应用和实践，帮助金融机构应对新风险，顺应新趋势，建设新局面。安

中国网

数字城市安全论坛：建设防护体系，保障健康稳定运行

8月26日下午，2021北京网络安全大会(BCS2021)数字城市安全论坛开幕。该论坛由中国电子信息产业集团指导，奇安信集团主办，中国电子云支持。论坛以“打造数字城市安全防护体系 保障数字城市健康稳定运行”为主题，聚焦数字经济时代下的数字城市安全建设，深入探讨如何打造数字城市安全防护体系、保障数字城市健康稳定运行。

此次数字城市安全论坛由奇安信集团安全运营中心总经理万京平主持。中国电子信息产业集团有限公司总经理助理、数字办常务副主任、中电互联党委书记、董事长朱立锋，中国电子云副总裁陈磊，赛迪顾问研究业务总监高丹，长沙市数据资源管理局党组书记、局长张武，香港警务处网络安全及科技罪案调查科总警司罗越荣，嘉兴市大数据中心主任屠勇刚，奇安信集团副总裁张龙分别分享了自己的思考和见解。

中国电子信息产业集团有限公司总经理助理、数字办常务副主任、中电互联党委书记、董事长朱立锋表示，开展城市数据治理要在保证数据安全的前提下激活数据要素，在推动数据要素市场化配置的工作中，我们坚持“打造‘一库双链’，培育三级市场”的核心理念，着力打造“数据金库”基础设施，充分利用“数据元件”可析权、可计量、可定价的价值属性，积极推动从数据资源到数据元件、再从数据元件到数据产品的“两次赋能”，加快培育数据资源、元件、产品三级市场，实现数据“资源化、资产化、资本化”的三次“蝶变”。

中国电子云副总裁陈磊在会上表示，城市信息化和数字化已经全面铺开，建设数字城市，要坚持安全为先，选择更可信的数字基础设施。中国电子云基于新一代可信云架构，围绕数字城市健康发展提供安全、绿色、先进的数字基础设施，护航数字中国建设。

赛迪顾问研究业务总监高丹表示，未来城市高

质量发展的基本动力仍将是工业化和城镇化，而经济高质量发展、产业高效协调将为城市工业化和城镇化注入动力，因此，网络安全问题现已成为城市数字化建设关注的焦点。赛迪顾问建议未来可从顶层设计、持续运营、评价体系、人才培养四方面着手加强城市数字化转型过程中的网络安全建设。

长沙市数据资源管理局党组书记、局长张武分享了他在城市网络安全运营中心的经验。他表示，随着信息化发展越深入、对网络安全的要求就越高，建立城市网络安全运营中心就是要给整个城市修城墙。集合智慧城市、重点行业和关键信息基础设施领域网络安全建设的发展核心，能有效地监控城市网络安全状态，守护城市网络安全运行，让城市具备自适应、自主和自成长的安全能力，提高城市网络空间安全的整体防护水平。

香港警务处网络安全及科技罪案调查科总警司罗越荣分享了香港警方是如何采取积极措施打击科技犯罪，其中在 2021 年网络安全和科技犯罪的行动重点清单中提到以下四点方法：提高公众对于网络犯罪的认知，加强与法律执法机构或不同利益方之间的合作，加强协调与共享专业知识，采取更加积极主动的措施去调查与打击网络犯罪活动。

嘉兴市大数据中心主任屠勇刚在会上分享，围绕浙江省数字化改革总目标，应坚持系统安全观，按照“全面覆盖、深度融合”的安全理念，强化政务网络安全体系，同时在日常安全运营中，围绕“云、网、端、数据、业务”的安全风险，全面落实网络安全“三同步”要求，构建与数字化融合的内生安全防护能力，强化数据要素安全保障，提升网络安全防护与实战对抗能力，打造坚实的网络安全底座，保障数字化改革的安全稳步推进。

奇安信集团副总裁张龙表示，城市安全运营中心兼顾监管机构和政企客户的网络安全诉求，采用集约化、标准化的建设方案。运营通过整体评估、环比分析、同比分析了解安全情况。同时，通过运营推动改进，基于当前的安全状况及未来的趋势，持续推动管理及技术的改进。用产业落地、产教合作的办法，建设数字城市的网络安全运营能力。安

谭晓生：中国网络安全技术趋势分析

近 20 年间中国的网络安全产业经历了翻天覆地的快速变化，无数技术的创新与迭代支撑着整个行业产品、服务、模式像时间的指针一样不断向前发展。

8 月 28 日，在 2021 北京网络安全大会上，北京赛博英杰科技有限公司董事长谭晓生进行了《网络安全技术趋势分析》分享，以下为分享全文：

今天我来给大家分享一下我们对网络安全技术趋势的分析。

网络安全基础框架

我从事了 30 多年的软件开发和网络安全相关工作，今天首先为大家输出的是一个网络安全研究框架（框架图详情见下页）。我们把网络安全分成六大基础安全领域，分别是端点安全、网络与基础架构安全、应用安全、数据安全、身份与访问管理及安全管理。这六大基础安全领域基本上是以安全产品形式提供。

但仅仅提供产品，用户并不能很好地做好安全，所以通过安全方案与集成、风险评估、安全运维、渗透测试、应急响应，红蓝对抗、攻防实训与靶场、培训与认证，安全意识教育与安全众测这十大安全服务来辅助用户把安全工作做好。

同时和产品、服务相交的还有四大通用技术理念，分别是威胁情报、数据安全与治理、零信任与开发安全，他们应用在各个基础安全领域并贯穿在安全服务之中。

同样，现阶段还有四大新兴的应用场景，分别是云安全、工控安全、移动安全和物联网安全。

六大基础安全领域、十大安全服务、四大通用技术理念、四大新兴场景最终要解决的是各个行业的安全问

题。在过去这 20 年，中国的网络安全市场里面形成了六大行业，他们是安全的主要客户，分别是运营商、金融、能源、医疗、卫生、教育和公检法司。

端点安全

下面我们逐一来看，首先是端点安全。端点安全最近这些年有什么变化?

首先端点的类型逐渐变多，从过去的桌面电脑逐渐有了移动终端，到现在万物互联有了很多物联网终端。最初的终端安全是从杀毒开始的，20 世纪 90 年代有各种各样的杀毒产品，最近几年开始由 EPP 演化到 EDR。原因是什么呢? 在移动终端里面装杀毒效果就大打折扣，要在物联网终端里面装杀毒软件这事儿简直无从做起，所以这时候基于终端的检测和响应（EDR）就能够去帮助大家解决终端的问题。端点上的探测、云端协同的终端安全检测和相应的处置，都在逐步被解决。

技术上有什么变化?

第一，引擎的变化。和传统的杀毒相比，现在的引擎从“基于规则”发展到了“基于 AI”。2009 年在全世界开始出现基于 AI 的引擎，如 360 的 qvm、趋势科技的引擎等。经过十几年的发展，现在基本所有的安全公司都在采用 AI 引擎。

第二，判定方式的升级。从过去基于代码特征来杀毒，现在逐渐变成基于用户行为进行恶意判定；从由本地判定，到云和端结合来判定，再结合威胁情报来进行防护。

第三，过去 20 年发展起来的终端安全管理市场（包括准入、各种三合一的管控等），这些也归入到终端安全管理的范畴之内。现在我们已经把终端安全管理扩展到了移动终端和物联网终端层。

第四、主机安全曾经是一个很古老的细分领域，叫主机加固，最近几年随着云的流行出现了越来越多的 HIDS、HIPS 这方面的应用，比如，像青藤云、椒图、

安全狗都是这方面的新兴供应商。

第五，可信计算终于到了落地的时候，尤其在物联网终端，我们需要标识身份，并对它们之间的通信进行加密。

第六，终端侧的漏洞管理。在过去，出现漏洞我们都简单地告诉用户打补丁，但实际上用户在很多时候很难对他的系统打补丁，尤其是物联网终端，终端侧的漏洞管理技术会给客户提供智能化的管理，很好地解决了这个问题。

网络安全

第二个大领域是网络安全，网络安全是在终端安全出现之后的第二个大市场，一直到现在它都是网络安全市场主要的收入构成部分。那么从防火墙到下一代防火墙，IPS、IDS、各种各样的全流量采集和分析设备、SDWAN/SASE 这种服务模式的出现，到 DNS 安全的兴起、蜜罐的复兴……这些产品逐渐演化的过程中，技术是如何发展的?

首先，从最早防火墙的第三层检测和防护，发展到应用层（第七层）的检测与防护，这是第一个技术进步。第二，VPN 正在面临升级和换代，零信任网络就是可以替代 VPN 的下一代的产品，下一代 VPN 产品就是基于零信任思想的网络安全控制手段。第三，在网络安全方面也存在由规则引擎到基于大数据 AI 引擎的技术变化。第四，过去防火墙都基于静态的本地规则去做，今天采用了协同联动和威胁情报去进行封堵。

应用安全

应用安全过去大家讲的比较多的都是 Web 安全，除此之外，其实还有邮件安全、API 安全等领域。应用安全上，WAF 是一个存在了 10 多年的产品，长亭科技在 WAF 近些年的发展是一个很好的例子，在 WAF 这个红海市场里他开辟了一个新的体验点，主要是由 WAF 过去表达式的防护到基于语义分析的防护，效果可以说是做到了全球领先的水平，这是一个技术进步带动老产品更新很好的案例。

在最近两年 API 安全又开始被提出来， API 的未来

其实在今天还没有完全的被确定下来，API 安全既可以用于解决攻防问题，也可以用来解决数据安全之类的合规问题。我个人预测 API 安全到未来的几年时间会具体的落地，具体会落到什么样的领域，解决什么样的问题，我们还需要拭目以待。

数据安全

数据安全是一个非常大的品类，我们从数据安全和数据安全治理这两个角度来看。

数据安全现有的产品大多是基于数据审计和数据加密方面，但是今天我们所面临的数据安全问题其实远远超过这些领域。在这里我简单列了一下，比如，数据脱敏问题，数据要发挥更大的价值在于共享，这里就会涉及隐私等数据安全问题，数据脱敏及隐私计算都是用于解决数据共享问题的产品。

数据访问的时候有各种的权限控制问题，这个在讲身份控制的部分也会涉及。还有大数据平台的安全性，大数据平台基于各种各样开源系统，在设计初期没有考虑太多安全问题，一般认为只要数据能“算”就可以了，但在数据变得越来越敏感的时候，大数据平台的各种安全机制就变成了一个强需求。还有像数据备份与恢复，就是对付 WannaCry 这种勒索攻击的一种手段。

在数据安全领域的技术进步也有很多，如在隐私计算方面。昨天安全创客汇我们就讲到现在至少有 15 家新的创业是在做隐私计算这个方向，有做联邦计算、多方计算、同态加密等。

身份与访问管理

身份与访问管理其实也是一个传统的大市场。

我们先看 IAM。在过去的这些年，IAM 首先用的是用户名口令这种传统的手段，大家都知道这种方案效率低，对用户不友好，但是到今天我们其实还没有办法完全地抛掉用户名和口令。后来我们有了多因子认证，现在零信任网络架构也试图从一定的角度去解决这个问题。

那么从 PAM 权限管理这个角度，我们经历了从 IBAC（基于身份的权限访问控制）到 RBAC（基于角色的访问控制），到 ABAC（基于属性的安全访问控制）。在今天这个产品仍然在逐渐的完善过程中。

还有在云服务越来越多的情况下，IDaaS 也变成了世界上非常主流的一个潮流，虽然中国和国外之间的发展趋势会略不一样。

还有这两年非常火的零信任，零信任在国内是一个热词，很多的创业公司都要打零信任的标签，零信任有一个非常重要的部分就是和身份访问管理有关的，它很大程度上解决的也是身份和访问控制的权限问题。

安全管理

在安全管理这方面，在过去这几年我们解决了几大问题。一个是数字资产的发现与管理，一个是从 2015 年国内安全行业开始建设的威胁态势感知，可以说是完成了从 SIEM 到提前感知的进程跨越。

还有 SOC，可以说过去很长一段时间里，把 SOC 这个产品做成功的公司特别少，到今天 SOC 的自动化水平得到了极大地提升。现在我们也能看到 SOAR 的演进，SOAR 在目前还不能算是一个获得成功的产品，但在未来，我们对它给予很大的希望，因为在人类技术进步的过程中，提高自动化水平，减少对人力的消耗是我们追求的终极目标，尤其是在安全人员远远不足的当下，只有通过提高自动化和智能水平，才能减少对于人的消耗。

在漏洞管理方面，漏洞管理以往的方式是打补丁，但是很多用户系统很难去打补丁，这种情况下，漏洞化管理成为了一种新的方式，通过访问权限的控制，通过一些防火墙的规则设置可以去解决打补丁的问题，什么时候该装补丁？什么时候可以采用其他方法去解决？这都属于安全管理方面我们获得的一些进步。

安全服务一开始大家都比较容易接受的首先是渗透

测试服务，过去安全公司都会准备一个渗透测试团队，先上去把用户打穿了，然后再卖产品进去。到今天我们有专业的安全公司的安服人员，还有各种众测公司，包括最近国家信息安全测评中心搞了一个众测的项目。

还有像 MSS 和 MDR 这种安全托管服务，在 2021 年各大安全上市公司的年报里面都会提到自己要做 MSS 或者 MDR，这里面的原因主要是我们整个社会都在做数字化转型，需要保护的系统和财产越来越多，但是我们的网络安全人员一年只能培养出来几万个，离安全教职委说的“我们需要 140~150 万的安全人员”这个数差距太大，很长时间都难以去满足这个要求。另外，人员设置也是要花钱去养护团队的，通过安全的云服务方式，才是能够低成本为用户解决问题的一个手段。所以对 MSS 和 MDR 这两个服务我们是非常坚定地看好，实际上开展相关业务的公司的经营效益也很好。

电子取证其实也是非常重要的一个安全服务，系统遭到入侵了之后，有专门的安全取证团队能帮你做取证服务，最终能够变成“呈堂证供”。

四大通用技术理念

刚才说到了四大通用技术理念，首先要提的就是零信任。零信任现在的基础组件其实就是一个微隔离，一个 SDN，一个 IAM。现在各种创业大赛里面号称是做零信任的公司特别多，其实零信任是一个思维方式，它会应用到很多传统的安全产品甚至服务里面去。比如，现在非常热的 SASE 里面也包含了零信任的应用。

再看数据安全治理与隐私保护，其实数据安全治理是解决数据安问题的一个有效方法，它首先有数据资产发现，我要先知道我有什么样的数据资产，其次能对我的数据去进行分类和分级，然后再去做各种权限控制；还要对数据进行加密，让别人入侵之后也无法拿走；数据分享的过程中还要脱敏，再加上传统的数据库审计防护、数据防泄漏等方面的需求。其实数据安全治理是一个非常复杂多样的工作，在内部它可以再分成很多细分内容，而在数据安全整个的工作中，今天的解决方案都处于非常早期的阶段，所以我们认为数据安全未来会是一个非常大的赛道。

数据安全技术主要的发展变化来自于从一开始是对数据进行静态的防范，今天我们要对于流转的数据去做安全管控，因为数据不流动起来，它的价值无法真正的发挥。第二点我们由过去的明文计算，到现在有了各种隐私计算，不管是联邦学习、安全多方计算还是同态加密，都是用来解决隐私计算问题的一种方法。还有我们在过去对数据标密的时候采用人工标密，现在随着数据量的膨胀人工已经无法满足需求，这就产生了数据的自动分类和分级。

在高级威胁发现方面，最近的两年各种解决方案和产品的大赛里我们看到非常大的比例是基于全流量分析的方案。2020 年我们做市场分析的时候发现，做 IPS/IDS 这两款产品的提供商在减少，但是基于全量分析的 NTA 厂商在非常快速的增加，并且应用了人工智能技术、沙箱技术等。从基于引擎的扫描到基于沙箱的检测，从人工的日志分析到 AI 的全流量分析，这都是在高级威胁发现方面的技术进步。

开发安全是随着开发左移的思想发展的，意思就是人们解决安全问题不是在产品最终要提交的时候再交给安全团队去测试，而是在开发过程之中就采用各种各样的交互式自动化的工具支撑来帮助开发者尽早发现漏洞。像悬镜安全、默安科技，都号称自己是一个 DevSecOps 公司，提供 SAST、IAST、DAST、SCA 等各种管理工具，分别解决静态安全扫描、动态的安全扫描、交互式安全扫描和源代码的成分分析等。

还有一个是 Fuzzing，Fuzzing 其实是 20 世纪 80 年代末学术界提出来的，但最近几年开始越来越广地得到了安全界人士的应用。现在 Fuzzing 到的一个问题就是要从专业人士应用变成普通开发者就能用，怎么形成自动化的漏洞挖掘工具，在开发过程中能帮助客户去找出来协议上和代码上的漏洞，这类产品的整个发展还是

要有自动化的工具来落地和支撑。

总结：下五洋捉鳖 上九天揽月

最后从总体上总结一下网络安全技术发展的趋势，在这里我放上了一张太极图。在 RSAC 等各大全球安全会议上，老外在演讲的时候也经常拿中国的太极图举例子，虽然我不知道他是不是真正理解太极图的意思。

在过去几年间我们看到有几个趋势，一个是安全的管理越来越细，从过去管一个终端的安全，然后到网络边界上的安全，再逐渐深入到代码的运行过程做了什么行为，再到后来的比如 API 安全关注到每一次的系统接口的调用，越来越细节。对数据也是，我们从过去用一台服务器做权限控制，到在服务器内部去分清楚它是哪个数据库，到现在要能分出哪条记录。这种越来越细的趋势，我们把它叫作“下五洋捉鳖”。

第二个就是“上九天揽月”，意思就是说虽然基于细节的管理我们的能力确实在提升，但依然是不够的。比如，像这次的新冠病毒，我们正好可以看出来中医和西医之间的区别，西医就是越搞越细，细到这个病毒的表面蛋白是什么，分子结构是什么，它到底是怎么感染人体的，该用什么样的疫苗，用什么样的药物去治疗它。但是这样越往下剖得越细，其实工作负荷是很大的，病毒这个东西是不是真的能被解决也是存疑的，比如很快就出现变异病毒了。那么中医的玩法不同，类似于不管你什么病毒，在中医看来都是癌症，中医通过把你的身体的机制调动起来，提高免疫力，让你身体的免疫力自己去把病毒干掉，不管是什么病通过这样的方式都可以来进行一定程度的防御。

像在网络安全里面，我们从更宏观的角度去看，不管是态势感知还是 UEBA，都是试图跳出细节，在掌握更大信息量的基础之上，通过找到一个更高层的规律来解决问题。

另外，在讲网络安全的趋势的时候，我们要知道网络安全领域没有一放出来就能解决所有问题的“独门大招”，且往往需要一个很长的过程。拿 Fuzzing 来做例子，在 1989 年的时候就有学者提出来这个概念，但在后面将近 20 年时间里都没有得到非常广泛的认同和应用。直到最近 10 几年时间高效 Fuzzing 工具的出现能够让专业人士开始用起来，今天我们再把它变得能让更普通的用户能够使用，整个过程从创意到产品应用要花费几年的时间。在这几年时间之内，大厂会不断的跟进，创业公司也会不断的跟进，最后往往会形成一个新技术，但它不是谁家的独门武器，而是多家公司都会具备这样的这种技术。所以在网络安全的技术演进上面，我们看到的是一个渐进的趋势，从一个创意最终到变成用户真正能用的产品，再快也得两三年时间，而且最后往往是逐渐迭代式的演进的这样一个过程。安

雷锋网

BCS 2021 技术峰会：攻与防的角力 经营安全推动网络安全技术变革

作为 BCS 2021 三大峰会（战略峰会、产业峰会、技术峰会）中的压轴峰会，技术峰会吸引了全球网络安全技术爱好者的热切关注。在今年峰会上，Forrester 副总裁、集团研究总监 Laura Koetzle（劳拉·科茨勒），北京赛博英杰科技有限公司董事长谭晓生，Kryptos Logic 高级威胁情报分析师与恶意软件研究员，WannaCry 破解者 Marcus Hutchins（马库斯·哈钦斯），复旦大学计算机科学技术学院副院长杨珉，美国俄克拉荷马大学助理副校长、讲席教授 David S. Ebert（大卫·伊尔伯特），北京大学大数据分析与应用技术国家工程实验室常务副主任袁晓如，蚂蚁集团副总裁韦韬，清华大学－奇安信集团联合研究中心主任段海新等发表了主题演讲。安全牛总编辑、国际信息系统审计协会（ISACA）中国专家委员会副主席陈伟作为主持人出席了技术峰会。

勒索病毒、供应链攻击，威胁侧的变化莫测

2021 年似乎一开始就是不平静的一年，在全球网络安全领域也充满了变化和挑战。从去年年底 SolarWinds 供应链攻击事件开始，有两个关键词一直充斥着人们的眼球，一个是供应链攻击，另一个是勒索攻击。值得关注的是，奇安信威胁情报中心已监测到多起安全公司被入侵造成的供应链攻击事件。

甚至，这二者开始出现了结合。今年 7 月 2 日，企

Forrester 副总裁、集团研究总监 Laura Koetzle（劳拉·科茨勒）

业管理软件供应商 Kaseya 被曝出旗下产品 KASEYA VSA 软件存在漏洞，已被 REvil 黑客勒索组织利用攻击，并造成其大量客户因此关闭服务。

“他们并不在乎黑进了哪家公司，他们只在乎能够花费最少的代价获取最多的收益。” 劳拉 · 科茨勒在演讲中一语道出了供应链攻击流行的原因，由于攻击目标往往处于供应链的上游，因此通常具备“攻其一点，伤及一片”的特点，尤其是攻击那些使用较为广泛的软 / 硬件产品。

劳拉 · 科茨勒说，SolarWinds 事件告诉我们，不要觉得供应链攻击离你很远，即便你不知名，但如果你有很多知名的客户，你依然具备极高的攻击价值。并且，攻击者为了达成攻击目标，通常会在目标中潜伏很长时间，从而植入恶意代码。为了应对这种攻击方式，组织机构应该尝试使用零信任架构，用于将每一次访问的安全风险降至最低，同时应当建立软件资产清单，便于清晰掌握软件供应链所面临的风险，即便发生攻击，也能在最短的时间内做出正确的响应。

但遗憾的是，大多数组织机构并没有明确掌握他们所使用的软件面临的风险，尤其是在引入开源软件的时候。由于开源软件使用的广泛性，给了大量攻击者以可乘之机。

根据奇安信发布的《2021 中国软件供应链安全分析报告》显示，在奇安信代码安全实验室分析的 2557 个国内企业软件项目中，平均每个软件项目存在 66 个已知开源软件漏洞，最多的软件项目存在 1200 个已知开源软件漏洞。其中，存在已知开源软件漏洞的项目占比高达 89.2%；存在已知高危开源软件漏洞的项目占比为 80.6%；存在已知超危开源软件漏洞的项目占比为 70.5%。

“多项开源组件受到高危漏洞影响、松散的开源社区管理难以有效推动漏洞修复，以及开源代码的漏洞补丁部署状况混乱，是造成开源代码面临的漏洞威胁巨大三个主要原因。”杨珉解释到，“面对这些不足，我们希望通过挖掘开源组件漏洞、增强开源漏洞信息，以及评估漏洞补丁状态等方面的工作去解决，尽管在这个过程中我们遇到了漏洞挖掘效率低、漏洞库信息不完整、补丁部署管理混乱等方面的困难。”

当然，饱受漏洞问题困扰的绝非只有普通的开源软件或者其他商业软件，互联网核心协议的漏洞问题同样不可小觑，由于使用更为广泛，其危害性甚至更加巨大，2014 年曝出的 OpenSSL 心脏滴血漏洞仿佛就在昨日。

“互联网基础协议的小问题常是互联网的大问题。”清华大学 – 奇安信集团联合研究中心主任段海新强调，

清华大学 – 奇安信集团联合研究中心主任段海新

作为互联网基础协议领域的安全专家，段海新又一次在技术峰会上，分享了他在该领域的最新研究成果。他说：“经过长期的研究和攻防实践，我们发现了互联网基础协议漏洞的一些显著特征，基础协议的漏洞影响范围很广，但想要运用自动化的方法来挖掘或者寻找漏洞却十分困难。并且，这些互联网协议漏洞绝大多数都是逻辑漏洞，甚至许多漏洞是多个系统组合在一起才出现的，需要多个系统组合在一起才能发现。”

与此同时，作为近年来威胁侧的另外一个“明星”，勒索病毒也一直保持着很高的活跃度，甚至是触发企业应急响应流程的最主要威胁。“勒索软件通常不再侵扰消费者系统，而是企图感染整个企业网络。”马库斯·哈钦斯介绍了近年来勒索病毒攻击的变化趋势。这主要是因为感染一家企业，要比同时感染数十万台设备要容易得多，并且相对个人消费者而言，企业支付赎金的意愿更强。马库斯·哈钦斯强调，勒索病毒的防范不仅仅是一个技术问题，仅靠提高安全性、增加安全预算是无法解决的，需要在金融、法律及网络安全等领域开展多方合作。

Kryptos Logic 高级威胁情报分析师与恶意软件研究员、WannaCry 破解者 Marcus Hutchins(马库斯·哈钦斯)

AI 可视化与平行切面，防护侧的技术变革

魔高一尺，道高一丈。奇安信集团董事长齐向东在 26 日战略峰会上谈到，只有煞费苦心地经营安全系统，才能保障经营活动安全运转。经营安全是对网络安全的动态掌控，只有让安全能力动起来，不断循环升级，才能破解复杂难题。

对于网络安全技术的发展趋势，谭晓生针对端点安全、网络安全、应用安全等网络安全所有技术领域，展开了非常深入细致的分析。从防火墙到下一代防火墙、从 IPDS 到 NTA 和 NDR、从 SD-WAN 再到 SASE，以及安全管理和安全服务，推动了整个网络安全防护水平向前发展。

在所有用于网络安全的技术中，机器学习、可视化与平行切面等技术的应用，逐渐走进了大众的视野。

大卫·伊尔伯特表示，尽管深度学习已经在很多领域取得了成功，但它不是万能的灵丹妙药，目前也还没能最大化发挥它的价值，因此很多人都认为深度学习远

北京赛博英杰科技有限公司董事长谭晓生

比现在大有可为。他说，人们需要创造可视分析、可视化和人机协同决策环境，来帮助大众充分利用现有的所有数据源，并且把垂直领域的知识整合到可视分析系统中，改进分析流程，并且基于数据和先进分析，做出更高效的决策。

袁晓如也表达了这样的观点。他认为，智能新时代的可视分析是沟通数据、人与社会的桥梁。虽然机器初步具有分析、预测能力，但人类在复杂事物认知、常

北京大学大数据分析与应用技术国家工程实验室常务副主任袁晓如

识和创意的能力机器不能匹敌。他通过情报文本报告、舆情传播以及与奇安信团队合作的媒体新闻转载分析等可视化案例，指出通过设计有针对性的可视化界面，把人和机器结合起来，可以大大提高人类的知识认知能力。安全领域面临复杂的博弈，可视分析可以更好地帮助决策者理解复杂的数据场景，作出相应的对策。大数据、人工智能和计算能力是计算机科学拉动社会前进的三架马车，可视化可以帮助人类更好地驾驭计算和数据。

同样是与数据打交道，数据治理在拥有海量数据的今天显得更加重要。随着网络安全与数据安全逐渐深入到业务本身，数据安全治理与日常业务的开展经常会出现冲突。如果有一个平行空间，能够让业务部署维度与安全部署维度做到正交融合——两者既能融合为一体，又能独立解耦，各自独立发展，对于安全行业的发展来说将会是一个重要变革。

“安全平行切面体系（安全切面）是一个安全基础设施，通过嵌入在端管云内部的各层次切点使得安全管控与业务逻辑解耦，并通过标准化的接口为安全业务提供内视和干预能力。”韦韬给出了安全切面的概念。能够预见的是，在数据爆炸的 DT 时代，安全平行切面体系的引入，能够有效地推动数据感知覆盖、数据链路血缘高精度分析上产生新的突破，以解决数据治理面临的精确度、覆盖度、保鲜度等深水区的严峻挑战，并且在 App 隐私管控、数据分类分级、数据主体确权，以及数据输出防泄露等数据治理关键工作中起到重要作用。安

蚂蚁集团副总裁韦韬

YNET 北青网

BCS 2021 聚焦“安全经营” 齐向东首提实战化态势感知

“强大的认知能力能帮人们把握事物基本规律、判断事物发展方向、构建自身与世界的关系。网络安全的认知能力也是如此，只有及时看到威胁、揪出威胁、阻断威胁，才能确保安全能力行之有效。” 8 月 26 日，在 2021 北京网络安全大会（BCS 2021）开幕式及战略峰会上，奇安信集团董事长齐向东表示，经营安全是对网络安全的动态掌控，只有让安全能力动起来，不断循环升级，才能破解复杂难题。而实现动态掌控的第一个重要能力，就是认知能力，只有构建实战化态势感知，才能全面提升认知能力。

态势感知“单打独斗”不具备认知能力

“态势感知”，最早从军事领域兴起的概念，如今成为网络安全行业中最热门的领域之一。从美国、日本，到中国，各网络大国都纷纷将态势感知上升到国家战略高度。

2016 年 4 月 19 日，习近平总书记在全国网络安全与信息化工作座谈会上指出：“要全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”他强调，“没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是‘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’在里面，一旦有事就发作了。”

从 2016 到 2020 年，随着《网络安全法》和《国家网络安全战略》的相继出台，态势感知获得了空前重视。传统网络安全厂商和新兴的初创企业都在加大对态势感知的投入，同时在演进之中，这些产品根据实际场景的不同，逐渐进行了分化。

齐向东指出，“目前的态势感知主要分为三种：一种主要用于企业内网，我们称之为运营类态势感知；一种主要用于实战演练，我们称之为攻防类态势感知；还有一种主要用于监管机构，我们称之为监管类态势感知。”

然而，目前这三类态势感知主要以基础运行为主，靠他们单打独斗都不具备全面的认知能力，与实战性态势感知系统有很大差距。齐向东归纳了三个方面：

首先，以基础运行为主的态势感知，不具备实战性，

告警不全，不能追踪溯源，不能快速定位问题；其次，覆盖面不够，多数只覆盖信息化系统，没有覆盖生产业务系统，只覆盖总部和部分重要的二级部门的网络，没有覆盖三级、四级末端的网络；最后，对接入设备监管质量不高，比如，终端上对更广泛的物联网设备没有形成有效监管，对网络设备没有监管到端口和功能的配置，对服务器监管更加粗犷，对云、数据库、计算平台和应用系统也没有有力的监管。

形成实战化态势感知 才能提升认知能力

在瞬息万变的网络战场上，有利战机稍纵即逝，更早发现敌人，更先了解对方的行动计划，更有力地指挥调度全局，才能赢得胜利。类似在网络空间的复杂防对抗中，态势感知系统也需要能快速感知到威胁，将各个系统进行协同，汇总信息掌控全局，协调资源快速处置。反之，不具备实战能力的态势感知，无法保护用户的网络安全。

齐向东表示，只有将运营、攻防、监管这三类态势感知有机协同在一起，形成实战化态势感知，才能全面提升认知能力。三类态势感知能有机协同，需要构建统一的计算平台、标准和运营系统。有人把态势感知等同于安全大脑，这是不全面的。它是大脑（包括五官）、四肢和武功的三合一。大脑是监管态势，能看见威胁；四肢是运营态势，能揪出威胁；武功是攻防态势，能阻断威胁。

“实战化态势感知，和国家保护关键信息基础设施的理念要求是一致的。”关键信息基础设施的保护，可以分为监管层、行业层和运营层。奇安信的实战化态势感知系统能为这三个层级提供针对性的态势感知、监测和响应能力。

近年来，奇安信一直在大力打造研发平台，先后发布了“鲲鹏”“诺亚”“雷尔”“锡安”“川陀”“大禹”“玄机”“千星”等八大研发平台，同时还有十多个安全应用平台正在抓紧研发，这些平台已经掀起一场研发效率革命。通过平台化战略，奇安信实战态势感知拥有了把安全设备横向打通的核心能力，将安全产品所需的共性核心能力平台化、标准化，能把这些产品有效连接起来，实现协同联动。

态势感知领域 奇安信持续领跑

根据多家第三方机构的分析报告显示，奇安信在态势感知领域一直处于领先地位。2020 年 3 月数世咨询发布的《网络安全态势感知能力指南》显示，奇安信在技术创新力和市场执行力双第一。同时，奇安信监管类态势感知平台入选家工业信息安全发展研究中心公示的"2020 年人工智能优秀产品和应用解决方案拟入围名单"。在 " 安全牛 " 对外发布的《2020 网络安全态势感知应用指南》报告中，奇安信集团入围年度代表性厂商，同时有 5 个行业代表性案例入选，在数量和覆盖领域等方面，在所有入围厂商中位列第一。赛迪顾问报告显示，奇安信态势感知与阿全运营平台（NGSOC）产品连续 2 年在中国安全管理平台市场占有率 NO.1。

在态势感知技术创新方面，2021 年 4 月，奇安信天眼联合申报“APT 攻击检测与预防”项目荣获 WSIS 冠军奖。而为态势感知提供全量数据关联分析能力的奇安信“大数据流式分布式关联分析引擎 Sabre”，则成功斩获 2021 数博会领先科技成果奖。

在国家级重大活动网络安全保障，以及实战攻防演习中，奇安信态势感知承担了指挥平台、威胁检测平台、监控分析平台等关键角色。2021 年，奇安信态势感知先后参与了全国两会、建党 100 周年、世界人工智能大会（上海）、第 44 届世界遗产大会等多个重大活动，以及数百场实战攻防演习活动，提供了网络安全监测与指挥保障。尤其在多个重要部委、多个重要城市，奇安信态势感知一直是国家级重大活动网络安保的独家支撑平台。安

HC360慧聪网

数据安全与治理论坛成功举办 数字经济发展应注重安全治理能力

8月27日下午，在2021北京网络安全大会（BCS 2021）上，由鹏城实验室、国家工业信息安全发展研究中心联合主办，以“建数据安全体系、护数字经济发展”为主题的数据安全与治理论坛顺利召开。论坛邀请了一众研究机构、企业代表、安全厂商共同探讨，《数据安全法》出台后，各行业不同的业务场景下该如何用技术保障数字化发展与安全的平衡，如何解决好数据安全领域突出问题，提升数据安全治理能力。

中国工程院院士方滨兴受邀出席会议并发表了致辞。方滨兴院士表示，基于“数据不动程序动、数据可用不可见”的隐私保护新技术理念，提出可信计算平台——AI靶场，它通过调试与运用环境分离的数据分析关键技术，在保证数据隐私安全的同时最大限度发挥数据价值，为数字经济高质量发展筑牢安全屏障。

国家工业信息安全发展研究中心保障技术所所长李俊认为，当前国内工业数据安全的问题主要体现在三个方面：全局战略的数据安全意识薄弱，数据管理和分级分类防控能力不足，数据安全防控技术手段欠缺。对此，应加快贯彻落实《数据安全法》，建立工业领域的重要数据清单目录，加强重要数据保护，建立工业数据的安全评估认证体系，规范化开展我们工业数据安全的风险评估、防控能力评估和跨境安全评估，加强监督检查。

联通数字科技有限公司总裁李广聚表示，目前数据合规问题正逐渐跃升为大数据产业发展的主要风险，涵盖从数据采集到数据应用的全链条。数据安全合规是数据流通的基础和前提，联通数科牢记央企的责任与担当，树立正确数据价值观理念，坚持“安全合规是生命线、安全事件零容忍、敏感数据不出门”的三大安全原则，基于DSG、DSMM、DCMM等打造了联通大数据安全体系，获得了国家部委及行业的认可。

国家电网有限公司大数据中心安全质量与合规部大数据安全处副处长刘圣龙强调，数据安全体系建设要遵循“依法合规、智能防御、可管可控、可审可溯”的原则，坚持业务场景全覆盖、业务过程全监测、安全管控全流程、人员管控全到位、安全防护全周期的“五全”管理思路，构建数据安全防护架构，提升数据安全防护水平，促进数据安全流动共享，保障数据业务安全稳定运行。

中国民生银行信息科技部安全规划中心副处长李吉慧从当前数据安全面临的威胁、数字化时代金融数据安全防护体系、对未来金融数据安全保护工作的思考与展望三个方面，阐释了“数字化时代金融数据安全防护体系实践”的主题演讲，并呼吁金融机构应进一步加强协同合作，采取数据安全管理与技术措施综合施治，以应对不断出现的新问题和新挑战。

奇安信集团副总裁韩永刚提出，数字化时代，数据伴随着业务进行流转，与传统安全不同，数据安全与业务逻辑必然有更多的交互，更深刻体现内生的理念。构建大数据安全防御体系，不仅要考虑到抵御威胁与攻击的数据实体与计算环境的安全防护，还要将基于零信任架构的动态细粒度访问控制能力与业务应用结合，实现对数据流转的精确控制，做到“主体身份可信、行为操作合规、计算环境与数据实体有效防护”。除了我们经常使用的数据全生命周期的视角，也要特别注意业务与数据流转视角，数据安全能力设计要梳理“数据脉络”，将安全能力和举措嵌

入进去，这就需要一套能力框架进行指引。为此，奇安信发布了“奇安信数据安全能力框架”，以及“数据安全概念运行构想图”，以助力数据安全管理升级与防护体系构建，勾勒了面向未来的体系化建设路线。

德勤中国风险咨询合伙人肖腾飞表示，数字化时代，大数据、人工智能、移动化、敏捷、创新，未来最大的威胁可能还是网络安全风险。对用户和企业而言，围绕以数据为中心的安全管控至关重要。应依托信息安全的体系管理，转变为聚焦核心数据安全风险扁平化管理，打造安全中台，为安全数据化及运营服务提供底座和抓手，适应烦杂的合规要求推动自动化能力。

鹏城实验室研究员、哈工大深圳－奇安信数据安全研究院副院长韩培义就“如何平衡隐私保护与数据挖掘的冲突”这一问题，提出了破局隐私保护与数据挖掘相悖的方法——模型加工场。他表示，模型加工场是一种用于加工模型的安全可控分析平台，基于“数据不动程序动、数据可用不可见”的新理念，在保证隐私的前提下进行数据价值挖掘。

全知科技 CEO 方兴表示，《数据安全法》合规要求下的数据安全解决方案，应以分类分级为纲，以数据风险为领，结合数安法，重塑可落地、有效果的数据安全治理。其中，分类分级为纲是指建立数据分类分级保护制度、鉴权全流程数据安全管理制度、对数据实行分类分级保护、确定重要数据具体目录、列入目录数据进行重点保护；数据风险为领则是指，数据风险评估、数据风险监测、数据安全事件应急处理。

御数坊创始人及 CEO 刘晨对通过数据治理打造数据底座的质量安全双保险提出了行动建议。他认为，应盘点数据资产、构建数据资产目录，建立数据认责、实现“人－数”协同，覆盖全域数据、提升数据质量业务价值，技术与管理并重、构建数据安全治理体系，采纳智能化技术、实现数据治理提速增效。毕竟加强数据治理能力，提升数据质量，保障数据安全，是数字化转型与数据资产价值创造的坚实基础。

深圳昂楷科技有限公司磐石研究院院长官文兵在演讲中表示，新形势下的数据安全守护已经从外围防守转向贴身守护。官文兵现场分享了昂楷科技在数据安全治理上探索的新模式，这套解决方案包括数据资产发现、数据资产授权、In-session 控制、资产应用追踪四方面，成功实现了实施和运营快速见效、应用场景和安全措施灵活、颗粒度和过程细致的运营效果。

“数据”已经成为数字经济时代下新的生产要素，是国家的基础性资源和战略性资源，也是重要生产力。BCS 2021 数据安全与治理论坛的举办，有助于构建出更富有创造性和前瞻性的数据安全体系，提升数据安全治理能力，从而帮助政企数字化转型和移动化建设。安

36Kr

隐私计算：可信应用实践与挑战

2021 北京网络安全大会，由蚂蚁集团主办、隐私计算技术联盟承办的「隐私计算技术及应用发展高峰论坛」于 8 月 27 日开启，洞见科技合伙人、数据智能总监王湾湾受邀出席论坛，发表了题为《隐私计算技术可信应用与实践》的演讲。

此次高峰论坛演讲的嘉宾还有蚂蚁集团共享智能部总监袁鹏程、华控清交副总裁黄斌、瑞莱智慧联合创始人刘荔园、富数科技副总裁卞阳、蓝象智联合伙人 & 首席算法科学家毛仁歆。

在《隐私计算技术可信应用与实践》演讲中，洞见科技王湾湾展示了隐私计算的发展历程及应用现状、隐私计算面临的可信安全问题、无第三方的联邦学习（NTP-FL）、区块链增信隐私计算、隐私计算面临的挑战及未来发展方向等五个方面内容。

王湾湾介绍，隐私计算，全称隐私保护计算（Privacy-Preserving Computation），是指在提供隐私保护的前提下，实现数据价值挖掘的技术体系。

隐私计算是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。它能够在保障数据隐私安全的基础上，实现数据「价值」的流动与共享，真正做到「数据可用不可见」。

安全多方计算、联邦学习和可信执行环境等隐私计算技术经历了一段时间的探索发展，现在已可以成熟应用到政务、金融和医疗等行业领域。

然而，隐私计算虽然被认为是目前解决数据安全和隐私保护的技术最优解，也依然面临着应用中的可信安全问题。例如：

1. 如何验证隐私计算协议本身是安全的，防止数据泄漏？

2. 如何验证隐私计算的实现与申明的计算协议是一致的？如何验证交互的数据未包含敏感信息且无法推测出原始数据？

3. 隐私计算需要参与方之间的多轮通信，如何保障通信信道安全？

4. 如何防止参与方进行数据投毒、模型投毒？

5. 在有第三方的架构中，如何防止第三方被攻击或与其他方共谋？

6. 如何保证隐私计算的结果数据未泄漏敏感信息？

针对上述问题，王湾湾详述了洞见科技基于技术信任的隐私数据安全保护体系（SAAAAS）是如何通过可信的技术手段来保障数据的计算安全。该保护体系包括安全计算、安全建模、使用授权、存证审计、访问控制、身份鉴定等六大维度。

针对第三方可信风险问题，隐私计算行业内厂商在分别进行理论研究和技术实践，例如，研究无可信第三方的联邦学习算法、引入区块链作为增强多方信任的工具。

王湾湾在论坛上讲解了洞见科技自研的无第三方的联邦学习（NTP-FL），并对比了有无第三方联邦学习方案的优劣。

有第三方联邦学习方案，优势是数据提供方之间可不建立通信，第三方与所有参与方建立通信，劣势是存在第三方与其他方合谋的风险导致数据泄漏，适用场景为带监管性质的机构可作为可信第三方。

无第三方联邦学习方案，优势是不存在第三方信任风险问题，劣势是需参与方之间两两建立通信，在参与方为三方及以上时，商业应用协调成本高，适用的场景为无合适的机构作为可信第三方。

关于区块链增信隐私计算，王湾湾表示，区块链技术为隐私计算带来更多信任，区块链的发展是建立在加密技术、分布式网络技术上的，它经历了数字货币 1.0 时代、智能合约 2.0 时代，现正在进入大规模应用 3.0 时代。

区块链技术结合隐私计算，共同打造技术信任链接服务、数据和智能「孤岛」，实现互联互通新格局。

对于隐私计算面临的挑战和未来的发展，王湾湾说，除了在安全可信方面的挑战，隐私计算还面临着性能瓶颈和互联互通壁垒。

性能瓶颈制约隐私计算大规模落地应用，目前正在通过算法优化和硬件加速等来改善，如优化算法流程设计，降低通信次数及通信量，优化加密计算效率，也可以结合硬件加速技术（如 GPU、FPGA、ASIC 加速）实现特定算法来实现硬件加速计算。

平台互联互通壁垒阻碍了隐私计算助力数据流通，目前行业内通过建立互联互通标准和增强互联互通实践来应对，如北京金融科技产业联盟、中国信通院等多家组织机构正在通过建立标准或测评来积极推动互联互通建设，而越来越多的厂商之间也在推进平台之间的互通，洞见科技在技术侧已与蚂蚁集团、锘崴科技等多家机构实现了「管理系统」和「算法协议」两个层次的互通，正在朝着第三层次「计算原语」互联互通的方向迈进，在业务侧也与多家金融机构实现了互联互通上的合作。

国家政策给隐私计算的发展带来利好。数据要素、数据安全相关的法律法规，为隐私计算技术在数据流通应用中的落地提供了指引，推动了行业良性发展。安

IT168.COM

聚焦行业数字化建设 BCS 2021 工业互联网安全论坛在京召开

8月27日下午，在2021北京网络安全大会上，以“助力数字化中国建设，筑牢工业互联网安全防线”为主题的第三届工业互联网安全论坛成功召开。作为业内极具权威性的全球安全行业交流平台，国家工业信息安全发展研究中心副主任郝志强、国家工业信息安全发展研究中心产业促进所研究总监赵慧等领导出席并发表重要演讲，与奇安信集团副总裁孔德亮、吴俣等企业嘉宾共同探讨如何进一步夯实工业互联网安全基础，提升行业安全治理能力。

近年来，工业互联网已成为数字化中国建设的重要应用领域，工业互联网的发展将显著改变我国工业生产的形态和流程。活动伊始，国家工业信息安全发展研究中心副主任郝志强发表致辞。

会上，国家工业信息安全发展研究中心产业促进所研究总监赵慧对相关安全政策进行了解读。赵慧表示，我国高度重视工业互联网发展，深入实施工业互联网创新发展战略，工业互联网连续四年被写入政府工作报告中。安全始终贯穿在相关政策文件中，各地方也相继同步出台工业互联网安全政策文件，安全体系建设已取得阶段性成果。未来，随着网络安全产业发展创新，工业互联网安全保障能力将进一步增强。

浙江大学控制学院教授、工业控制系统安全技术国家工程实验室研究院冯冬芹认为，工业互联网的本质应是服务工业生产，用 IT 技术服务于现场生产控制。他表示，工业生产中工控系统面临不同类型的网络风险，如骚扰工控系统的勒索病毒、损毁基础设施的破坏型病毒等。目前，在工业生产中工控网络安全的防护至关重要，通过最新研发软 / 硬件安全体系，可以做到对病毒的准确识别和提前预警，通过预埋代码可及时阻断危害，保证生产安全。

随后，奇安信集团副总裁孔德亮发表了《“双平台一中心”驱动工业互联网安全卓越运行》主题演讲，与现场嘉宾分享了奇安信在工业物联网安全层面的思考与经验。孔德亮强调，基于多年来在大数据、威胁情报、防病毒、安全攻防、态势感知等方面突出的技术优势，以及实战中累积的全场景全链条的安全服务能力，奇安信提出“双平台一中心”的全新工业互联网安全体系框架，驱动工业互联网安全卓越运行。

目前，奇安信通过层次清晰、定位明确、融合联动的工业互联网安全产品体系和解决方案，已成功在能源电力、轨道交通、智能制造、钢铁、水务等垂直行业落地，打造了十余个行业标杆案例。

在工业互联网安全体系的探索层面，中国船舶工业综合技术经济研究院总信息师丁宇征表示，在我国工业互联网已成为新基建的主战场，现阶段工业互联网安全工作面临诸多挑战，低防护联网设备数量增长迅猛，高危漏洞呈明显上升趋势增长，以及工业数据安全、新技术融合问题、系统复杂性等带来多重风险，亟需构建弹性工业互联网安全工程，为企业设置多重安全防护系统。

聚焦能源行业互联网数据开放面临的风险挑战，全球能源互联网研究院信息通信研究生副所长、国家电网公司信息网络安全重点实验室主任张涛表示，做好能源行业数据安全，在贯彻国家数据安全法规要求的基础上应构建数据安全治理体系，强化数据业务场景的安全能力。同时，还要精细化电力数据资产管理，强化电力数据资产智能化识别，严格数据流动场景、多方数据联合的安全管控能力，精确提升业务数据安全审计能力，全面提升数据安全智能监测和处置能力。

石化盈科信息技术有限责任公司信息技术研究院院长索寒生发表题为《打造面向石化行业的内生安全工业互联网》的演讲，他表示，以石化行业为代表的传统产业已成为网络攻击的重点对象。目前，根据行业规划设计安全防护体系，结合石化行业工业互联网平台应用发展和实践，现已形成行业互联网平台安全防护系统构架。通过适合工业业务特征的综合态势感知技术，对工控系统层进式纵深防护，完善工业互联网的内生安全体系。

作为中控技术网络安全业务负责人，何有明为大家介绍了中控在工业软件领域的布局，生产管理层中可能遇到的网络安全痛点，以及在生产管理层网络安全领域的成果。此外，烽台科技副总裁王启蒙也出席了本次论坛，并发表《融合业务安全需求，助力工业企业数字化转型》的主题演讲。

据介绍，工业互联网安全论坛的举办，旨在探讨工业互联网安全防护的理论方法以及实践效果，为工业互联网相关企业提供参考，促进工业互联网安全生态进一步发展壮大。而作为本次论坛的主办方，奇安信在坚持技术创新、增强产品能力的同时，也会发挥龙头企业带头作用，将安全能力对外辐射给更多合作伙伴，共同完善工业互联网安全生态。助力数字化工中国建设，筑牢工业互联网安全防线。安

CSDN 全球最大中文IT社区

InForSec 网络空间安全国际学术成果分享论坛成功举办

8 月 27 日，北京网络安全大会（BCS 2021）议程进入第二日，由 InForSec 主办的网络空间安全国际学术成果分享论坛正式举办。本次论坛议题为“网络安全国际四大顶会学术成果分享”，来自加州大学尔湾分校的助理教授陈齐、蚂蚁安全对抗技术部负责人曲和、蚂蚁金服隐私计算高级算法专家王力等多位业内人士及学者，共同探讨人工智能安全及漏洞入侵防范等国际前沿技术研究。

会议第一部分的议题为“信息物理系统安全”。来自加州大学尔湾分校的助理教授陈齐指出，自动驾驶（AD）技术因其在驾驶安全性、效率和移动性方面的显著优势而一直受到国际追捧。在该技术中，AI 感知决策极为关键，它决定了驾驶决策的安全性，如避免碰撞和保持车道，因此其中的任何安全问题都可能直接影响道路安全。他分享了其最新研究，通过两个关键 AI 模块：感知和定位，发现多种可攻破工业级自动驾驶 AI 的新型物理层攻击（如激光雷达攻击、恶意形状的路面障碍物、路面污渍等），造成严重交通隐患。他还介绍了更广泛意义的智能交通中 AI 安全性的最新研究，尤其是车联网技术的研究。

近年来，指纹认证在移动设备越来越受欢迎，被称为最受用户青睐的身份认证方式。然而，在实际使用的环节中，它易受到展示攻击（Presentation attack）的威胁。对此，众多研究学者提出了基于软件和硬件的方法以防御展示攻击，这些方法关注更多的是指纹活体检测，无法防御指纹认证中被忽视的木偶攻击。

关于如何“使用行为特征技术增强指纹认证以抵御木偶攻击”，武汉大学国家网络安全学院博士生吴聪在会上分享了他们的设计方案——一种基于行为特征的指纹认证增强方案 FINAUTH。当用户在执行指纹认证的时候，通过分析指尖触摸（fingertip-touch）的行为特征，即可判断当前输入指纹的用户是否为合法用户。FINAUTH 仅依赖于移动设备上常见传感器，不会给用户带来额外的操作负担。

移动应用开发过程中嵌入了大量的第三方库，它们丰富了移动应用的功能，但是也引入了许多安全风险，如从移动设备及应用后端服务器窃取用户隐私数据。中国科学院大学博士生王基策研究揭示了一个新的严重威胁用户隐私的攻击向量——恶意第三方库攻击集成于同一应用程序中的其他第三方库，以获取用户隐私数据（Malicious Cross-library Data Harvesting）。通过检测 Google Play 市场上的 130 万个移动应用，发现“42 个恶意库从 16 个流行的第三方库中窃取数据，影响了超过 19000 个应用，研究进一步揭示了这种数据收集行为背后的地下生态系统，它们独特的数据收集策略及其重要影响。”

论坛第二部分的议题为“软件安全”，来自蚂蚁集团安全对抗技术部的林以，带来了题为《APICRAFT: Fuzz Driver Generation for Closed-source SDK Libraries（USENIX Security 2021）》的演讲。闭源 SDK 库的 fuzz driver 生成常常面临两大挑战：一是闭源 SDK 库仅有有限的信息可被提取；二是 API 函数之间语义关系复杂，但仍需要保证其正确性。为了解决这些挑战，他们提出了 APICRAFT，一种自动化 fuzz driver 生成技术。通过将

APICRAFT 实现为 fuzz driver 自动化生成框架，并使用来自 macOS SDK 的五个攻击面对其进行评估。在评估中，APICRAFT 生成的 fuzz driver 表现出比手动编写的更出色的代码覆盖率，平均提高了 64%。

开发者在调用 API 时，需要遵守软件库文档中所规定的约束。违背 API 的调用假设被称之为 API 误用，其会造成严重的软件安全问题。中国科学院信息工程研究所研究生吕涛研究了如何更加高效地检测 API 误用。考虑到自然语言处理技术的快速发展以及其在各个领域产生的显著效果，基于该技术提出了一套系统性的方法来自动化地提取调用假设并将其转化为验证代码，以发现与调用假设相违背的应用程序代码（即 API 误用）。

由于密态计算的复杂度高、通信量大，导致在实际应用中性能难以符合要求，蚂蚁金服隐私计算高级算法专家王力发表了题为《高性能隐私保护机器学习算法》的演讲，并介绍了如何结合机器学习和多方安全计算的计算特性，提升隐私保护机器学习的安全性和计算性能，在保证算法实用性的情况下，做到可证安全。

近年来，兴起以 AFL 为代表的 Coverage-based Greybox Fuzzing 技术。然而，AFL 在测试时会分配过多的能量（即种子变异产生的测试用例的数量）给执行高频路径的低质量种子，从而浪费了大量的计算资源。此外，当前研究领域对 Coverage-based Greybox Fuzzing 技术的调度算法方面的研究还不够深入。对此，国防科技大学计算机学院博士研究生乐泰提出了一种基于 Adversarial Multi-Armed Bandit 的变异式模型来对 Coverage-based Greybox Fuzzing 中的调度过程进行建模。并在 AFL 基础上实现了一款自适应能量节约型 Greybox Fuzzer——EcoFuzz。乐泰曾将 EcoFuzz 与其他 10 个工具在 14 个真实程序和 LAVA-M 上进行了对比测试，此次参会，他向大家分享了该实验结果，“相较于 AFL，EcoFuzz 能够在减少 32% 测试用例生成数量的情况下，达到 214% 的路径覆盖率。此外，EcoFuzz 还发现了 GNU Binutils 和其他软件中的 12 个漏洞。我们还扩展了 EcoFuzz 来测试一些物联网设备，并在 SNMP 组件中发现了一个新漏洞。”

最后，来自清华大学网络空间研究院博士生陈凯翔系统地介绍了现有的虚函数保护理论，指出当下的虚函数调用保护存在被绕过的可能性，并分享了结合真实程序和漏洞的调研结果。安

经营安全推动网络安全产品技术创新 近 20 款网络安全产品重磅亮相

8 月 26 日，以“经营安全 安全经营”为主题的 2021 北京网络安全大会 (BCS 2021) 在京盛大开幕。在为期三天的大会期间，每天都有多款网络安全产品和解决方案重磅发布，引领着网络安全技术发展。

多个“内生安全”行业落地成果发布

基于内生安全理念，新一代网络安全工程实践课程发布

为了推动人才培养侧和产业需求侧的有效对接，奇安信安全教育产品部面向高校推出了基于“内生安全”的新一代网络安全工程实践课程。

网络安全工程实践课程系列，第一批包括《企业网及其服务建设》《企业网安全产品集成》《企业网应用安全防护》《企业网安全运维》《企业网渗透测试》《企业网等保测评》《企业网安全运营》等几门课程，并通过安全项目管理的基本思想串联相关实训内容。

奇安信集团安全教育产品部解决方案负责人李向辉表示，新一代网络安全工程实践课程是对高校网络安全相关专业必修课的补充，帮助学生进行产业课程实践，这些实践课程，既培养学生技术能力，也培养学生非技术能力。课程采用项目制、情境式、任务驱动的教学方式，让学生成立项目小组完成任务，培养学生技术能力的同时全面培养学生非技术能力。

对高校来说，网络安全工程实践课程充分地体现了以岗位工作任务为导向的职业能力培养模式，既可以满足高职院校项目实训的需要，也可以满足本科院校培养学生网络安全领域的复杂工程实践能力的需要。

5G 网络风险敞口扩大，奇安信推出 5G 安全解决方案

自从 2019 年我国进入 5G 商用元年开始，5G 在行业应用实践的广度和深度不断提升，在医疗防疫、工业互联网、车联网等领域涌现众多优秀案例。随着 5G 的蓬勃发展，5G 安全也越来越受到国家和各行各业的高度重视。

5G 安全架构是对 4G 的延续和增强，提供了更好的空口安全、更强的隐私保护等，但这不意味着 5G 网络就安全了。5G 系统依旧是通过网络承接，各种新型设备接入网络，将带来新的攻击方式和漏洞类型。此外，5G 在接入网和核心网采用了网络切片、网络功能虚拟化等一系列新技术，也将带来新的安全挑战。

针对 5G 安全面临的现状，奇安信基于内生安全的理念，将 5G 与安全能力进行融合，通过将安全功能内置到网元，使 5G 网络能自动免疫、主动防御、按需提供安全服务，最终达到 5G 网络的网元可信、网络可靠、服务可配的内生安全目标。

奇安信集团解决方案经理陈三强表示，内生安全理

念摆脱了传统安全框架以局部和外挂为主的缺陷，实现网络安全能力与信息化环境融合内生。基于内生安全理念，我们可以建立起覆盖端、边、云、网的全方位 5G 安全防护体系，打造面向各行各业的系统化 5G 安全方案。

《全球高级持续性威胁（APT）2021 年中报告》发布

在 TI INSIDE 生态联盟发布会上，奇安信威胁情报中心发布了《全球高级持续性威胁（APT）2021 年中报告》（以下简称《报告》），系统总结了今年上半年的主要攻击活动，及其背后所呈现出的 ATP 攻击新态势。

《报告》显示，2021 年上半年以来，被曝光的 APT 组织使用的在野 0day 漏洞数量陡然剧增，出现的频次之高历年罕见。APT 组织在野利用的 0day 漏洞数量超过 40 个，这在网络安全历史上堪称空前。随着网络武器威力和攻击规模的持续增大，今年上半年也许是近年来 APT 攻击活动最黑暗的半年。

《报告》指出，在野 0day 漏洞集中出现在多个平台，其中 Windows 操作系统、Chrome 浏览器、Adobe Reader PDF 阅读器等具有垄断地位的系统和产品均受

到了不同程度的影响。针对性地减轻在野0day漏洞风险，是现阶段抵御 APT 攻击的当务之急。

除此之外，展厅发布会上还发布了《疫情之下政企机构互联网访问风险报告》等趋势报告，以及网络安全威胁情报生态联盟成员授牌、奇安信集团与工业和信息化部人才中心战略合作等重要仪式。

立足安全运营 奇安信发布多项网络安全产品

27 日产业日下午，奇安信集团向大家展示了 Q-SASE 产品、云安全运营中心、边界安全栈新能力、零信任身份安全解决方案 3.0、开源卫士新版和数据安全能力框架等多个创新产品成果，为行业及政企客户带来了更多安全声音。

三大全新发布直击安全运营

“面对不断翻新的安全挑战，当前，信息网络安全行业亟需全新的安全设计思路和服务方式来重构安全体系，打造数字化发展的坚实底座。”中国信息通信研究院技术与标准研究所互联网中心副主任穆琰博在发布会致辞期间强调。

对此，奇安信正式发布安全访问服务 (Q-SASE)，

奇安信 Q-SASE 正式发布

基于 SASE 扩展架构和服务化模式，针对国内政府和企业分支机构互联及移动办公安全访问场景，通过安全防护体系和零信任体系协同进行的服务化安全运营。据奇安信 SASE 业务负责人王茜介绍，Q-SASE 安全访问服务基于 4 个统一的安全理念，即统一安全架构、统一防护水平、统一访问策略、统一运行管理，通过人、工具、流程、情报的协同服务，帮助客户完成安全防护、监测、分析、响应、处置的服务化闭环，为政企客户提供网络和网络安全的功能融合的统一安全服务。

据奇安信云安全事业部总经理孙立鹏介绍，奇安信云安全运营中心的核心能力包括三个维度，一是资产管理、脆弱性管理和威胁分析，二是风险维度，包括识别、分析和运营三个层次，三是关联分析引擎这一重要底座。这“3+3+1”，组成了奇安信运营中心的核心能力框架，实现云上安全运营自动化、实战化，为云上业务保驾护航。

此外，有研究机构统计，2020 年数据泄露总条数约为 360 亿条，数据泄露事件给企业造成的平均损失达 386 万美元。在数字化时代，海量数据需要通过流动交易来产生价值，数据伴随着业务和应用在不同载体间流动和留存，贯穿信息化和业务系统的各层面、各环节，数据流转过程中面临各种各样的风险威胁，这对数据安全防护提出了更高的要求。

面对数据安全的现状与挑战，奇安信正式发布数据安全能力框架 2.0，覆盖数据安全治理的不同阶段，帮助政企组织从基础环境安全、身份安全与访问控制、数据保护、检测与响应、审计与定责和备份恢复等方面构建数据安全防护能力。

奇安信集团副总工程师刘前伟认为，数据安全的全流程防护应基于数据应用场景、业务逻辑和数据流转，构建数据脉络，在不同环节做风险分析和威胁建模，将安全能力和举措植入到应用和业务中，与系统、应用和业务的各层级深度融合，在关键环节对重要数据做精准管控，将“零信任架构”与“数据安全防护体系”相结合，做到主体身份可信、业务操作行为合规、计算环境与数据实体有效防护，从“管理、技术、运行”来开展数据安全的治理与数据全流程安全防护工作。

三项创新升级覆盖多个领域

在产品发布活动上，奇安信集团副总裁吴亚东重新定义边界安全新模式，为大家带来了边界安全栈新能力的发布。当前，加密流量成为网络中主体流量，也给政企组织带来了新的安全挑战。为此，边界安全栈通过改变传统边界安全架构，重塑边界安全防护体系，为用户提供更加智能、动态的安全防护。

据吴亚东介绍，此次边界安全栈虚拟网元数量从 5 个增至 11 个，以满足客户日趋多样化的安全需求。同时，新能力全面提升了 SSL 解密性能，其异步调用、硬件解密、解密能力提升 10.6 倍，可解密加密流量 (支持 TLS1.3)，然后分别给到不同的安全设备进行安全处理，从而实现一次解密、多次安全处理，帮助政企客户轻松应对网络中加密流量被黑客利用不易发现、不同安全设备解密能力弱等问题。

边界安全栈新能力还增加了物理网元和虚拟网络的混合服务链编排，可将流量按照不同业务需求进行流量编排、引流和负载均衡，改变传统边界设备安全串接的模式，做到业务按需引流，设备上线下业务无感知。

在数字化业务、新技术的发展变化，以及远程办公等多重因素驱动下，数字化进程对安全提出了更高的要求，零信任理念和方法也在不断演进。会上，奇安信身份安全事业部总经理张泽洲正式发布奇安信零信任身份安全解决方案 3.0，其核心内容可概括为“零信任 123”，即基于“从数字化经营视角看零信任”的安全理念，通过零信任身份安全一套整体框架，构建策略驱动的零信任访问检控体系、数字化身份及动态策略管控体系两大能力体系，囊括零信任战略规划服务、建设咨询服务和安全运行服务三项支撑服务。

践行零信任，需要从数字化经营视角出发。张泽洲强调，零信任之路不可能一蹴而就，切忌将零信任简化或僵化，但也不可将零信任过度神化，一定要在规划牵引下，从能力和场景方面有序、持续地去构建。

与此同时，随着开源技术应用越来越广泛，开源软件也面临着来自安全漏洞和知识产权风险的威胁。为了帮助企业做好开源软件的治理，奇安信于 2019 年推出开源卫士，本次 BCS 产品发布活动现场，奇安信集团代码安全事业部产品组长刘岩带来了开源卫士全新版本，安全能力全面升级。

据介绍，奇安信开源卫士本次升级特性之一是全面覆盖软件生命周期不同阶段的成分分析，包含源代码、二进制制品、容器镜像等多种形态；第二个特性是漏洞情报升级，精准定位漏洞，多维度风险评级；第三个特性是文本级许可协议识别，支持常见开源许可协议风险检测，支持 2500+ 开源许可协议的精确识别。目前，开源卫士可在企业软件自研、软件内购等多种场景下发现和帮助解决开源成分的风险。

自动化威胁检测与响应多个实战化产品集中亮相

天眼新一代安全感知系统、云锁服务器安全管理系统、安全 DNS、SOAR、系统安全平台……8 月 28 日，在 2021 北京网络安全大会期间，奇安信多款实战化产品和解决方案集中亮相，从高级威胁检测、安全编排自动化与响应、网络资产攻击面管理及服务器安全、工业物联网安全和供应链安全等多个方面，帮助客户构建实战化网络安全体系。

聚焦自动化威胁检测与响应

威胁的检测与响应作为网络安全体系建设的重要环节，历来受到政企机构的高度重视。然而面对变幻莫测的攻击手法和善于伪装的恶意样本，检测与响应手段仍然需要不断创新。

在威胁检测方面，此次亮相的奇安信新版天眼上线了智能助理、高级阻断、沙箱防逃逸等多项功能，其中新版沙箱在延续原版本对恶意文件智能、精准检测的基础上，大幅度提升了系统性能和安全性，同时检测环境支持 macOS 和 Android 操作系统，使得威胁检测样本覆盖更全。同时，为了避免威胁样本逃逸现象，新版沙箱实现了 TLS/HTTPS 流量解密的功能，阻止恶意软件采用 TLS/HTTPS 对自身流量进行加密保护以躲避检测的情况。

另一方面，新版天眼还增加了云上安全感知系统的“云天眼”，帮助用户重点解决云上全网安全在东西向流量上的监控盲区，建立一套在“云”上的监测预警、威胁检测、溯源分析和响应处置能力的高级威胁检测平台。

针对恶意网络请求的检测，奇安信安全 DNS（QDNS）基于奇安信威胁情报中心商业威胁情报，能够对 APT 攻击、勒索软件、窃密木马、远控木马、僵尸网络、网络蠕虫、恶意下载、黑市工具、流氓推广等几十种网络威胁请求进行有效的检测和阻断。

在响应方面，作为安全编排自动化与响应的利器，此次亮相的奇安信 SOAR3.0 以实战化为核心，能够帮助企业和组织将繁杂安全运行过程梳理为任务和剧本，把分散的安全工具与功能转化为可编程的应用和动作，并且借助编排和自动化技术，将团队、工具和流程的高度协同起来，覆盖安全运行的防护、检测、响应等各个环节。总体来看，奇安信 SOAR3.0 能够将安全事件调查与响应操作的效率提高 10 倍以上；对于需要重复性持续性的操作，提升的效率更是数以百倍计。

另外，奇安信新版天眼上线了高级阻断功能，能够结合 250w+ 条威胁情报、3000+ 威胁检测规则，实现对威胁的智能化阻断。

实战化安全运行

随着网络安全实战攻防演习的开展，政企机构对于

BCS2021 成果发布系列活动主持人

检测与响应的重视程度日益提升，网络安全体系建设越来越完善，但网络攻击事件依然处于高发状态。资产不清、漏洞不明、情报缺失、流程不通等基础安全问题多年来一直困扰企业客户，没有对资产安全形成运行服务闭环流程，就难以满足当前安全运营实战化、体系化、常态化的要求。

系统安全并非一蹴而就，也不是加强某个环节就能解决的，需要提升整体的防护水平。对此，“系统安全运行构想图”强调，需要用数据驱动的实战化安全运行模式，打通资产管理、配置管理、漏洞管理和补丁管理等四大基础安全流程，环环相扣融入整个大运维环节，从而收缩攻击面、有效控制数字化运营的基础风险。

通过构建系统安全运行服务支撑平台，建立多源异构资产和漏洞数据的融合治理、统一管理，达到全面掌握自身网络资产真实安全状况的目标；同时，帮助政企客户实现流程的通畅 & 闭环，达到管理更有序的目的；平台自动化能力体现到实际运营工作中，让原本重复的安全运营工作变得更智能、更简单、更高效，让安全运行真正成为日常。从而建立与大运维深度融合的安全运营体系，为安全运营的常态化、实战化奠基。

另外，为帮助客户检验防护体系的有效性，奇安信此次发布的自动化渗透测试系统，在学习总结奇安

信攻击队的多年实战攻防经验基础上，自主研发了高级漏洞利用框架及大量漏洞利用插件，通过自动化完成信息搜集、社会工程、漏洞利用、权限提升、持续控制、横向渗透等渗透测试全过程，将传统“手工作坊”式的渗透测试转变为自动化标准化可量化的渗透测试体系。

常态化核心资产防护

作为存储机构核心数据的地方，服务器一旦被攻破很可能会导致大量敏感数据丢失或被窃，因此在网络安全体系里，服务器安全防护通常是最后一道防线，其重要性不言而喻。

基于服务器端轻量级 Agent 的云锁服务器安全管理系统，同时支持单机版、公有云和私有云的部署。通过统一的 Web 控制中心，RASP、IN-APP WAF 及服务器操作系统内核加固探针，实现对传统物理服务器和云服务器一致的风险排查、内核加固、已知威胁的精准检测和未知攻击的有效防护。

此次发布的新版云锁重点新增了针对无文件攻击、带外（OOB）攻击、恶意扫描、恶意文件上传等检测能力，对反弹 Shell、RCE 利用和 EDR 检测做了重点优化。

同时，云锁还创新性的在服务器安全领域引入了微隔离和零信任的理念，基于不同角度（端口、外连、文件、应用等）的白名单机制，以攻促防，从恶意流量“打点 -> 拿权限 -> 横向渗透”的攻击逻辑出发，实现不同阶段对高危行为的高效防护。

在工业安全方面，工业物联网是工业信息系统的神经末梢，直接影响着系统运行质量，保障工业物联网的安全就成为工业信息化发展的重中之重。针对工业物联网接入设备自身防护水平差，网络接入缺乏监测、感知能力，安全事件缺少有效技术处置手段，系统存在极大被远程入侵风险等问题，“天择”工业物联网接入安全防护系统，对入网终端进行精准、持续、严格的细粒度管控，确保接入网合法、合规、可信的同时，全方位掌控网络边界动态，及时、灵活、高效地处置安全事件，确保网络无风险运行。

体系化供应链安全

供应链连接了这个世界的每个角落，无论是物理空间还是网络空间，一个组织已经不能仅仅通过保护自己的基础设施来保护自己。在网络空间对抗不断升级、数字化加速转型、国家战略推动、开源代码被普遍使用的情况下，体系化的软件供应链安全建设势在必行。

据奇安信威胁情报中心发布的《全球高级持续性威胁（APT）2021 年中报告》显示，在愈演愈烈的 APT 攻击中，APT 攻击团伙攻击目标开始更加侧重于在供应链中负责提供服务的公司。例如，去年 12 月，黑客在针对网管软件提供商 SolarWinds 发动了供应链攻击，在软件更新包中植入了后门程序，全球超过 18000 家机构都受到了此次事件的影响；又如，全球航空电信协会 SITA——管理着全球超过 400 家航空公司的机票和旅客数据处理，便曾在今年 3 月宣布服务器被黑客通过高度复杂的攻击手段入侵。而在国内，奇安信威胁情报中心也曾监测到多起安全公司被入侵造成的供应链攻击事件。

供应链安全建设面向两个主要的场景：第一是用户视角的供应链安全管理场景；第二是开发者视角的供应链安全开发场景。针对这两大场景，奇安信提供的软件供应链安全解决方案，包括代码安全能力、软件空间测绘能力、感知与自主测试能力、自动化流程管理能力等四个部分。安

奇安信位居“2021年中国网安产业竞争力50强”第一名

6月16日，中国网络安全产业联盟（CCIA）揭晓
“2021年中国网安产业竞争力50强”。
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，
奇安信位居第一名。

“2021年中国网安产业竞争力50强”榜单

TOP15	公司名称	公司简称
1	**奇安信科技集团股份有限公司**	**奇安信**
2	深信服科技股份有限公司	深信服
3	启明星辰信息技术集团股份有限公司	启明星辰
4	华为技术有限公司	华为
5	天融信科技集团股份有限公司	天融信
6	腾讯科技(深圳)有限公司	腾讯
7	阿里云计算有限公司	阿里云
8	新华三技术有限公司	新华三
9	绿盟科技集团股份有限公司	绿盟科技
10	杭州安恒信息技术股份有限公司	安恒信息
11	三六零安全科技股份有限公司	三六零
12	亚信安全科技股份有限公司	亚信安全
13	中孚信息股份有限公司	中孚信息
14	杭州迪普科技股份有限公司	迪普科技
15	山石网科通信技术股份有限公司	山石网科

齐向东携最新著作《漏洞 2》参与“名人名书”活动

8 月 26 日，奇安信集团董事长齐向东携最新著作《漏洞 2》，参与 BCS 2021 “名人名书”活动。

《漏洞》（第二版）是齐向东在奇安信上市后对《漏洞》一书的升级更新，齐向东从专业角度，用简明易懂的语言盘点奇安信最新的网络安全思想，解读国家的新政策新法规，梳理未来网络安全行业发展方向。

《漏洞》（第二版）也是齐向东根据过去十几年的从业经历，围绕网络安全领域的本源、基本构成、关键要素和未来趋势，对网络安全产业的总结和思考。

BCS 大会已经成功举办了三届，从 2019 年的“聚合应变 内生安全”，2020 年的“内生安全 从安全框架开始”，到 2021 年的“经营安全 安全经营”，每一年的大会主题都引发了网络安全行业的广泛讨论，成为了行业发展的风向标。

“名人名书”活动是 BCS 大会的特色活动之一，以圆桌对话形式展开，特别邀请上海华与华营销咨询有限公司董事长华杉共同参与讨论。节目结束后举办的《漏洞 2》签赠活动”获得了热烈关注和积极反馈。

民警反诈小课堂走进 BCS 2021

网络诈骗肆意横行，全民反诈势在必行。2021 北京网络安全大会期间，一线民警进入 BCS 开设“民警反诈小课堂”，揭示最新的骗术手段，最有效的防骗技能。

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

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com


经营安全 安全经营
2021北京网络安全大会