CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance GREATER CHINA REGION

全球数字契约展望及数字安全报告发布

演讲人：李雨航 云安全联盟大中华区主席

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

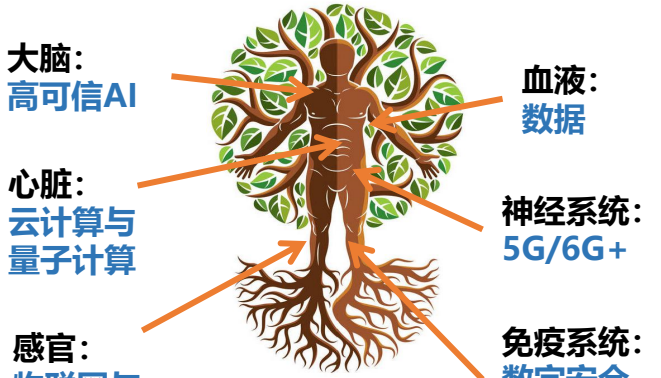
CONTENTS

数字时代的技术与安全

业务	. 生成式AI . 工业互联网 . 智能制造+ . 空间通信 . 三维全息 . 数字孪生 . 新智慧城市 . 自动驾驶	技术	. 云原生 . AR/VR计算 . 量子计算 . 6G and Beyond . 人工智能 . 区块链 . Web3.0 . 生物识别芯片	安全	. 安全领域的可信AI . 区块链/智能合约 . 零信任软件定义边界 . 5G/6G 安全 . 数据安全与隐私计算技术 . 量子安全

物理世界与虚拟世界的实数融合，数字技术是基石，数字信任和安全决定坚固度

枝叶:数字业务应用场景



根干:数字技术基础设施

对照物理世界 - 数字世界的安全威胁

潜在世界性威胁与灾难需要国际合作共同对应，在数字领域需要建立全球 “数字信任，共同安全”

共享开放、自由和安全的数字未来

联合国秘书长于 2021 年 9 月发布了《我们的共同议程》报告。提出将在 2024 年 9 月的未来峰会上通过技术轨就全球数字契约达成一致。该 **数字契约** 涵盖了包括政府、联合国系统、私营部门、民间社会、学术界和个人在内的所有利益攸关方。全球数字契约将成为“所有人共享开放、自由和安全的数字未来的共同原则”。

- 数字包容与连接
- 互联网治理
- 数据保护
- **数字信任与安全**
- 网络人权
- 人工智能及其他新兴技术
- 全球数字公共资源
- 加快实现可持续发展目标

全球数字契约建议书

全球数字契约是一个国际合作的框架，数字安全是全球数字契约的重要组成部分，旨在确保数字环境的安全、隐私权的保护和数字技术的可持续发展。

CSA大中华区此前向联合国提交了“**全球数字契约建议书**”，围绕标准、合作、权益、应用四个方向提出行动建议，重点关注数据保护和整体数字安全。现建议已被联合国采纳，在全球数字契约加入**数字可信与安全**相关内容。

包容《全球数据安全倡议》的CSA大中华区的全球数字契约建议被联合国采纳
https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission-CSA_GCR.pdf

数字技术与数字安全是建设数字中国的两大能力

2023年2月末，中国中央、国务院印发的《数字中国整体布局规划》首次提出数字中国建设的整体框架，将数字基础设施和数据资源体系作为数字中国建设的两大基础，明确了建设数字中国对于推进中国式现代化的核心地位。

规划提到强化数字技术创新体系和数字安全屏障两大能力，**数字安全新域包括：原生安全、数据安全、网络安全、隐私保护、5G安全、元宇宙安全**，迫切需要提升我国在数字安全领域的人才储备和创新能力。

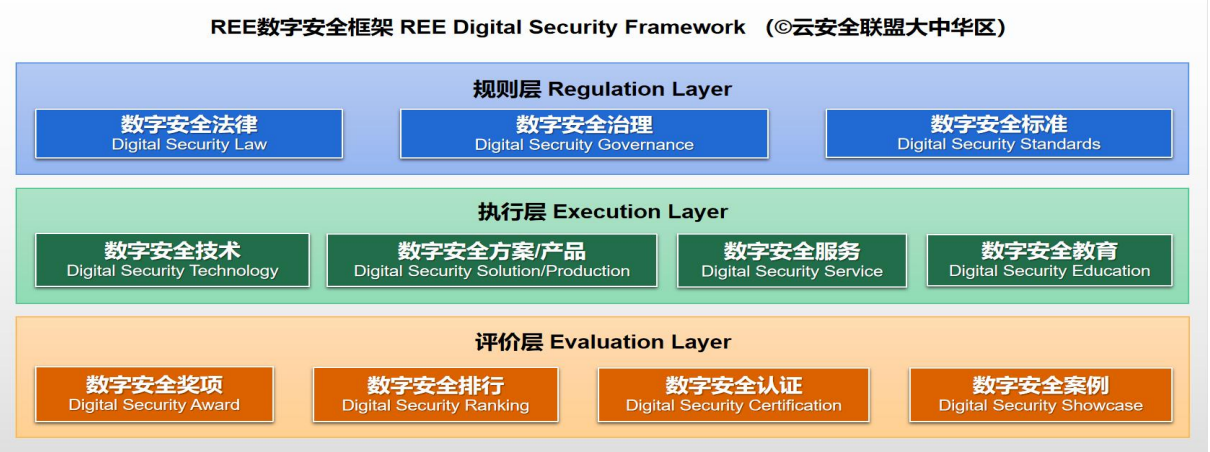
CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

CONTENTS

数字安全框架

REE数字安全框架 是云安全联盟大中华区于2022 年 3 月 11 日正式发布的数字安全的定义的重要组成部分。共分为规则层、执行层和评价层三层。



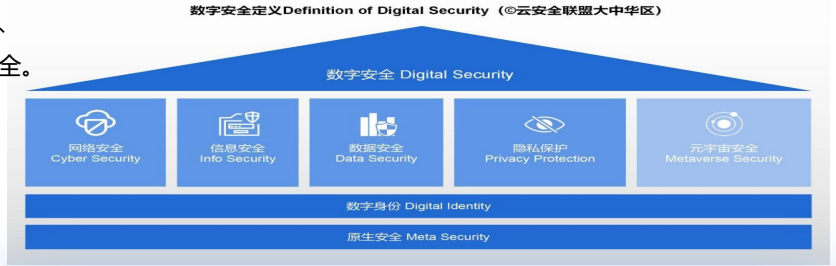
《全球数字安全报告》正式发布

《全球数字安全报告》为数字安全领域提供了一个国际前沿的新视野，帮助人们构建更加安全的数字环境。报告调研了全球数字安全各领域的现状，总结了优秀的实践、流行的技术和公认的数字安全提供商，帮助读者了解全球数字安全的发展概况。

数字安全: 网络安全的升级

数字安全的定义： 是指在数字时代与数字化相关的一切安全要素、行为和状态的集合，既包括保障数字经济的安全性，也包括将数字技术用于安全领域。数字安全以数字身份为核心，以原生安全为基础底座，涵盖了信息安全、网络安全、数据安全、隐私保护等领域或场景，并可扩展（如元宇宙安全）。除此之外，数字安全还包括利用数字技术保障数字基础设施的物理安全。

- **网络安全：**保障网络系统的硬件、软件的安全；负责人是CSO、CTO等
- **信息安全：**保障一切有价值信息的安全；负责人是CISO、CIO等。
- **数据安全：**保障数据全生命周期的安全与合规；负责人是CDO、CIO、CISO、CSO等。
- **隐私保护:** 保护用户的隐私与个人信息；负责人是CPO、DPO等。
- **数字身份：** 作为连接安全与业务的基座，提供所有的人、数字人、物、设备等的数字标识、认证、访问全生命周期管理。
- **原生安全：**是指下一代互联网原生安全，包括云计算、大数据、AI、5G/6G、IoT、区块链、量子计算等新兴技术所涉及的系统的原生安全，它是数字安全的底座，需要硬件信任根的支持。



数字安全框架首发 | 数字经济腾飞，数字安全护航

数字时代的新一代数据安全

- **原则：遵循“数字安全框架“基于零信任理念**：“永不信任，始终验证”理念和ABCDE 5大原则；
- **标准：**新一代数据安全：格式、协议、技术；
- **技术：**密控双态实现数据的安全可信，密态保障数据的私密性，控态保障数据的完整性、可用性和可信性；
- **范围场景：**

① 覆盖全生命周期和全环节，支持结构化、非结构化、半结构化和混合数据；

② 云网边端、动静用转、芯片/硬件/OS/中间件/应用/业务

解决数据确权、定价、交易、安全可信、合规监管的问题，保障数据充分流通和利用，发挥数据价值

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance® GREATER CHINA REGION

THANK YOU.