ZTE中兴

2030+网络内生安全愿景白皮书

2021 年 6 月

ZTE中兴 CAICT 中国信息通信研究院 中国移动 China Mobile 中国电信 CHINA TELECOM China unicom中国联通 奇安信

联合发布单位（排序不分先后）：

中兴通讯股份有限公司

中国信息通信研究院

中国移动通信集团有限公司

中国电信集团有限公司

中国联合网络通信有限公司

奇安信科技集团股份有限公司

作者与编审人员（排序不分先后）：

陆平	王继刚	王庆	葛林娜	杨红梅	冯泽冰
焦杨	张峰	于乐	邱勤	张弘扬	徐雷
马铮	张曼君	王姗姗	刘亚天	徐浩	呼博文
何国锋	金华敏	王锦华	黄铖斌	乔思远	罗海龙
李钠	苏硅	王飞	闫新成	郝振武 等	

前言

对于人类，刚刚过去的 2020 年，是个极为不平凡的年份。新冠疫情肆虐下，远程办公、在线教育等需求剧增，人类的生活方式发生了巨大改变，人类对科技尤其是移动通信网络的依赖更为紧密，网络空间升级为与天、空、海、地并列的第五人类活动空间，网络也正式成为基础诉求。

时代大变局下，新基建、数字化浪潮风起云涌，5G 正在以前所未有的速度迅猛渗透到千行百业，DOICT 加速融合汇聚，网络价值迅猛提升。“价值与安全恒成正比”，伴随着网络价值的迅猛提升，网络安全也被急剧推到前所未有的高度。新形势下，网络安全已成为产业和行业关注的焦点，安全需求已经成为网络的基础需求，也成为决定网络能否发挥最大化潜能和价值的关键因素，人类已正式跨入大安全时代。

从 1G 到 5G，移动通信网络一直呈明显代际发展效应。在 4G 以前，网络架构相对封闭，标准设计对网络安全的考虑基本满足和适应安全需求，网络实际建设时安全也主要依靠遵循标准来保障。5G 采用了全新 SBA 架构，引入网络功能虚拟化、网络切片、边缘计算等新型关键技术，大幅提升移动网络业务能力，支持增强移动宽带（eMBB）、海量机器类通信（mMTC）和超可靠低时延通信（uRLLC）等场景应用，更多的业务和应用也在向云化转移，从传统的人与人通信延伸覆盖到人与物、物与物之间的智能互联，使移动通信技术极快的发展和应用到更加广阔的领域。架构的开放、新技术的引入、云网的融合、各行业场景的渗透，不可避免的将其原来面临的安全风险交织到一起，安全问题复杂且充满不确定性。尽管 5G 标准层面相比 4G 已做了诸多考虑，但从市场诉求尤其是各垂直行业诉求和实际建设验证来看，还需要进一步的增强安全性。

与此同时，全球 6G 研究已经开启。6G 时代，天空海地网一体化，通信、超算、AI、感知等技术将高度发达，网络对基础信任机制、安全准入、存证与溯源、应急处置等需求将更为强烈。然而，传统 IT 领域的分散式、外挂式、补丁式安全防御模式已无法有效支撑。网络安全亟需在理念层面进行变革和创新，在设计构建时就要做出充分考虑。

2020 年 7 月，中兴通讯在 GSMA Thrive 面向全球正式提出了 5G 及未来网络内生安全的全新安全范式和安全理念，把网络与复杂精密的人类身体类比，借鉴人体生物学理念，为网络构建免疫能力体系，通过先天构建和后天生长，交付安全网络，并呼吁业界共同研究、积极分享，引起了业界强烈反响。

基于持续深度的探索实践，网络内生安全体系构建远非一朝一夕之事，需要长期的研究、思考、探索、验证、实践，本白皮书对 2030 + 网络架构进行了畅想，基于架构描绘了 2030+ 网络内生安全愿景，提出了统一的网络内生安全的定义，初步提出了网络内生安全需求，并设想了三个发展演进阶段，旨在引发业界的共同讨论与思考。

目前 5G 正在如火如荼的建设中，6G 研究尚在初始起步阶段，后续中兴通讯将联合业界共同完善更新报告，持续推进网络内生安全体系构建和潜能技术研究，护航并促进网络的可持续发展和演进。

社会发展驱动

可持续发展是人类的共同目标，移动通信网络重新定义了社会运转和人类的生活方式，这一点在 2020 年的疫情阴霾中显露无疑。通过网络，移动在线教育得以实施，孩子们教育有了持续保障；医生可以在线诊断病情甚至手术，病患仍有医可就；云上应用、远程自动化生产，保障工业等经济正常运转；远程办公、居家办公，保障就业收入；便捷的在线电商、买菜等，使得衣食住行有条不紊；未来，网络将会深度渗透赋能工业、经济、教育、生活等方方面面，这一切都需要安全作为基础和前提来持续保障。

技术演进驱动

在社会快速发展的驱动下，原有互联网、移动通信网、物联网、工业互联网等各种网络正在快速融合，如同大大小小的江河汇成大海，天空海地一体化成为必然。移动、云化、大数据、人工智能等技术赋予了未来网络强大的计算能力和智慧，安全的技术和新理念也层出不穷，零信任、软件定义安全、云原生、安全接入边缘服务等如雨后春笋般出现，传统的补丁式防御分散不成体系，远远不能发挥单项技术的潜能，也无法将新技术轨范在一个健康正向的发展道路上，因此，回本溯源，从顶层设计出发，建立“以一应万变”的安全体系，迫在眉睫。

商业模式驱动

如同人体，抵御疾病的第一主力军是免疫力，治疗疾病主要依靠免疫力加医生药品等科学治疗手段，免疫力对于人体如此重要。千百年来的人类经验表明，头疼医头、脚疼医脚的模式，只治其表、不治其本，最终会导向被疾病不断牵着鼻子走的局面，更无法从根本上预防和解决生病的问题，深入研究人体运作机能、免疫体系、能力，才有可能获得事半功倍的效果。这种智慧，对于网络同样适用。唯一不同的是，婴儿的免疫体系在母胎中就开始形成，而网络的免疫体系则需要智慧的网络专家来构建。未来，基于网络免疫体系，网络安全产业链和服务模式，将会呈现出医疗体系式的发展，网络安全的商业模式将真正实现健康、正向、可持续发展和演进。

内生安全最早源于生物领域的生物免疫系统，后来被借鉴和延续到科技领域、IT 领域，然后到 CT 领域，不过至今还没有形成统一标准的定义。内生安全能够为网络提供一个全新的安全理念乃至安全范式，启发以“向内转，向内思考”的视角来重新认知和看待网络安全问题。

借鉴人体生物学启示，汲取业界各领域的已有研究，面向未来，本白皮书尝试给出一个统一的“网络内生安全”定义：内生安全是网络的一种综合能力，这个能力由一系列安全能力构成，这些安全能力共同协作构成自感知、自适应、自生长的网络免疫体系。它必须在网络构建的时候同步构建，且能够在网络运行中不断自主成长，随网络的变化而变化，随系统业务的提升而提升，最终来持续保障网络及业务和数据的安全。

根据定义，网络内生安全应具备两个基本特点：先天构建和后天成长。先天构建，指安全需要与网络系统的设计与建设同步进行，如同一个婴儿，在出生时就已有基础的免疫能力，尽管这种免疫能力可能没有那么强大，或者因人而异，但必须有，好处是为后续的免疫能力成长提供了一个基础的机制和环境；后天成长，主要指安全能力对网络环境的适应和变化，如同婴儿出生后，在成长过程中，随环境等免疫能力也在不断适应和改变。

根据定义，网络内生安全具有两个核心功能：一体化、免疫。一体化指标准制定、顶层设计、建设、运维等阶段各层面需要将网络安全与功能网络全面融合，免疫指对恶意攻击、主动情报信息等的反馈和响应等完整闭环处理，同时保障网络数据全生命周期中的不可泄露、不可篡改和不可否认性。

畅想未来网络架构是描绘网络内生安全愿景的基础前提。作为人类第五活动空间，未来网络的架构将彻底向融合的新型一体化网络演进，这种融合体现在多个维度：DOICT 彻底融合、云网边端彻底融合、天空海地融合。未来，网络的概念也将发生变化，网络将成为由端、网、管理等共同构成的一个虚拟社会空间，被称为广义的网络体，而当前的传统网络则成为广义网络中的联结的一部分。未来网络架构将呈现扁平、分层、解耦等多个特性。关于未来网络的更深理解和展望，需要基于全新的视角进行抽象和审视。

未来，网络内生安全则作为广义网络的基础能力而存在。类似人体免疫体系，功能网络 + 管理 + 安全将共同构成具备内生安全的网络，安全既与网络深度一体化，又能独立成为完整的安全平面。统一的身份与信任体系将是未来网络及网络内生安全的基石，由边界、网元、全网三道防线相互协作，通过自感知、自适应、自生长等功能，实现具备一体化、免疫核心能力的内生安全能力体系。

图 1 未来网络架构

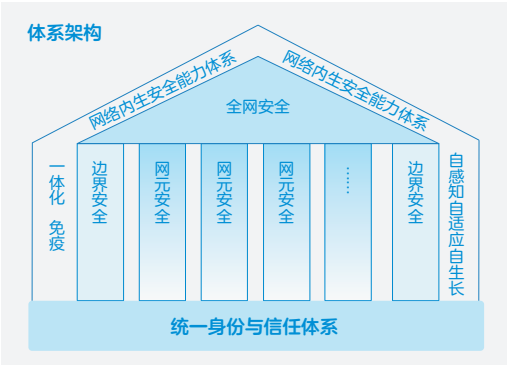

图 2 网络内生安全能力体系

从网络内生安全的功能看，网络内生安全将围绕网络架构及功能需求，支撑网络自身、行业，此外，安全自身也需要具备安全特质，因此，可以从业务的安全、安全的服务、安全的安全三大类，来综合概括对网络内生安全的需求：

业务的安全指内生安全能够保障基础层（网络、算力）、能力组件层以及应用层等各层安全，纳含软硬件设备及资源、传输、运行、大数据 /AI 等各能力组件安全、各行业场景（如工业、自动驾驶等）安全等需求。

安全的服务指内生安全面向应用层，内生安全能够提供安全能力、安全管理等安全服务，例如：旧业务下线时的安全收缩自适应、新业务上线时的安全能力自动化编排等需求。

安全的安全指内生安全能够保障自身安全。根据历史经验，安全与系统暴露面存在同向关联关系，因此，内生安全应遵从精简的原则，尽可能深度融于网络并尽量精简和优化设备，包括软件、硬件、端口等。

从网络内生安全自身的构建和发展演进角度，网络内生安全首先需要具备与网络深度的一体化，尤其是网络内生安全的先天体系，不能延后于网络体系，包括标准设计、顶层设计、方案设计、产品设计等。

从网络内生安全的衡量和演进看，网络内生安全还需要具备合理、可度量的分级和衡量标准。

考虑现有网络正处于多个异构网络的快速交织渗透和融合进程中，5G 及云网融合等也正在紧密的开展和进行，因此，从当前现状出发，面向未来，网络内生安全预计可以分为三个阶段来演进。

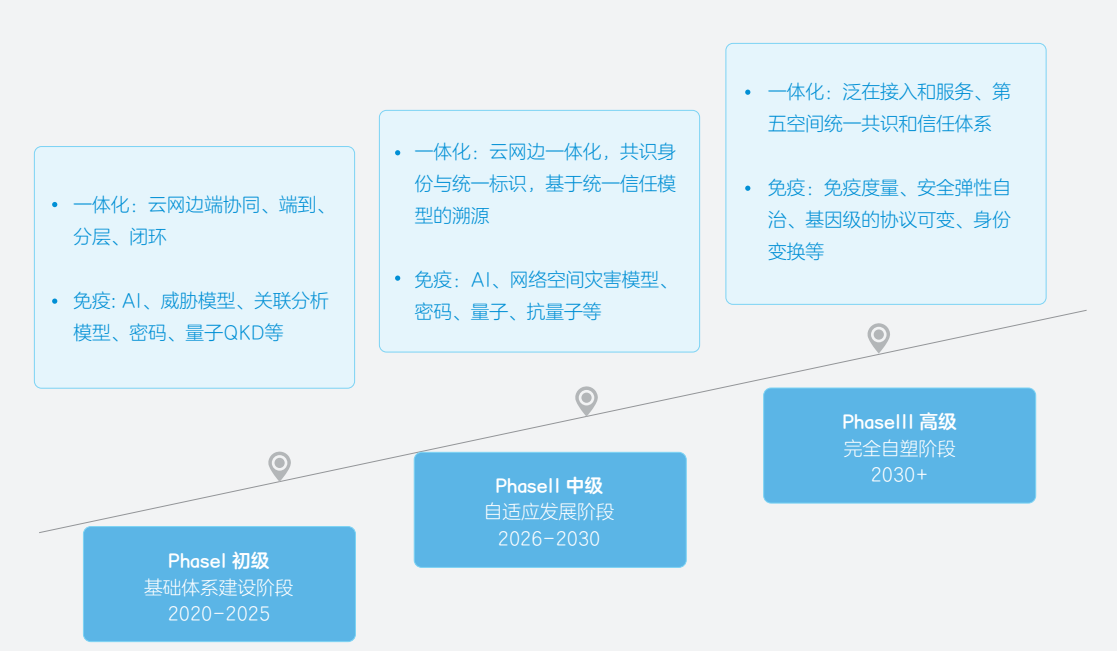

图 3 网络内生安全演进阶段

PhaseI （2020-2025）：这个阶段是网络内生安全的初级阶段，主要从业界网络现状出发，目标是初步构建一个完整的、没有严重缺失的基础内生安全体系，着重完成先天体系的雏形构建。从架构层面，该阶段主要以云网边端协同为特征，初步构建一个端到端、分层、闭环的内生安全体系，重新梳理当前的安全能力，基于软件定义、零信任等技术初步构建边界安全能力；基于软件定义安全、NFV、云等技术初步实现具备原子化安全能力的网元；基于密码、量子 QKD 等技术初步实现数据安全能力；基于态势感知、关联分析、APT 等技术初步构建和实现全网安全联动；基于 AI、威胁模型、关联分析模型等，初步进行免疫能力构建；初始阶段，网络安全将由外在的发散式、不可控的建设，转向收敛式、可规划建设；

PhaseII（2026-2030）：这个阶段是网络内生安全的中级阶段，主要基于 PhaseI 所构建的先天体系，着重进行后天自适应能力建设及发展，并反向促进先天体系的健全和成熟。从架构层面，该阶段主要以云网边端及云网边一体化为特征，发展和催熟内生安全自适应能力；基于共识身份和统一标识，通过构建基于分布式技术实现信任体系和溯源体系，进一步推进深层的全网一体化；在继续 PhaseI 的工作基础上，边界、网元等安全能力将向智能和协同方向深化；进一步基于 AI 和网络空间灾害模型等提升网络免疫能力。自适应阶段，安全需要部分人工干预，网络安全建设逐步具备一定的可控和收敛；

PhaseIII（2030+）：这个阶段是网络内生安全的高级阶段。经过 PhaseI 和 PhaseII，此时的网络内生安全应该已具备基本健全的先天体系和全网一体化的后天免疫能力，在第三个阶段，内生安全将反向促进网络架构的演进与变革，该阶段主要以端 - 网 - 管模式为特征，正式构成以共识体系为基石的第五空间一体化系统，该阶段将以支持协议级变化和身份变化等网络安全技能来适应安全诉求，网络的免疫能力也将能够量化度量，安全将能够弹性自治，基本不再需要人为干预。这也意味着网络安全将完成彻底的、系统化的收敛。

结束语

网络安全攻击者的目的与攻击手段在不断变化，所以安全的风险也是在持续不断变化，网络内生安全突破传统安全建设被安全攻击和风险牵着鼻子走的现状，提供了一种向内思考的解决之道，赋予网络以类似人体免疫“以一应万变”的安全能力，因此，网络内生安全也被称为变革性的理念、新的网络安全范式。

回顾历史，人类社会中的重大科技变革，远非技术单方面因素所决定，而是由社会、经济、哲学、技术、人文等多方面复杂因素共同推动形成，未来的网络及网络安全也如是，需要站在更高和更长远的角度来重新审视思考。人类的免疫能力经历了千百年的发展并仍在持续进化，刚刚萌芽的网络内生安全体系亦将任重而道远。中兴通讯将与中国信通院、中国移动、中国电信、中国联通、奇安信等伙伴密切合作，携手共进，持续躬身进行内生安全相关探索和实践，为护航网络可持续发展，扬帆奋进。

参考资料

1. 网络空间内生安全，邬江兴
2. An artificial immune system architecture for computer security applications.[J] . Paul K. Harmer,Paul D. Williams,Gregg H. Gunsch,Gary B. Lamont. IEEE Trans. Evolutionary Computation . 2002 (3)
3. 全球数字经济新图景（2020 年）——大变局下的可持续发展新动能，中国信息通信研究院 2020.10
4. 5G Security Report, CAICT, 2020.2
5. 中国移动 _2030 愿景与需求报告，中国移动研究院
6. 中国电信 _ 云网融合 2030 技术白皮书，中国电信集团
7. 中国联通 CUBE-Net3.0 网络创新体系白皮书，中国联合通信有限公司研究院
8. 新一代企业网络安全框架，奇安信集团，齐向东 乔思远
9. 5G 内生安全，何去何从？ 5G 及未来网络内生安全研究、构建与思考（上），中兴通讯，葛林娜 王继刚 王庆
10. 网络免疫系统，从靠近网络本质的设计开始。5G 及未来网络内生安全研究、构建与思考（下），中兴通讯，葛林娜 王继刚 王庆
11. 5G 云网融合内生安全 王继刚 葛林娜
12. 5G 及未来网络内生安全 中兴通讯，葛林娜 王继刚
13. 6G 大会 - 内生安全分级定义及关键技术 闫新成

ZTE中兴 中兴通讯股份有限公司 ZTE CORPORATION
地址：深圳市高新科技产业园科技南路中兴通讯大厦 邮政编码：518057
电话：+86-755-26770000 传真：+86-755-26771999 网址：www.zte.com.cn