基于内生安全框架的面向数字化转型的网络安全防御体系

A Network Security Defense System for Digital Transformation Based on Intrinsic Security Framework

韩永刚/HAN Yonggang
（奇安信科技集团股份有限公司，中国 北京 100044）
(QI-ANXIN Technology Group Inc. , Beijing 100044, China)

DOI：10.12142/ZTETJ.202206006
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221219.1325.002.html
网络出版日期：2022-12-20
收稿日期：2022-10-10

摘要：提出了网络空间安全领域的一种新安全体系设计、建设与运营思路方法。所阐述的内生安全，指通过内生安全框架方法，将网络安全能力与数字化环境进行融合内生，达到安全与信息化的深度融合与全面覆盖。以系统工程与企业架构的方法，结合内生安全理念，从体系化、全局化的视角，以能力为导向，可以构建动态综合的新型网络安全防御体系。

关键词：内生安全；系统工程；企业架构；网络安全能力

Abstract: A new method of design, construction, and operation of security systems in the field of cybersecurity is proposed. Through the intrinsic security framework, the cybersecurity capabilities and the digital environment are integrated, to achieve deep integration and comprehensive coverage with information technology. With the method of system engineering and enterprise architecture, combined with the endogenous security concept, and from a systematic and global perspective, a new dynamic and comprehensive network security defense system can be built.

Keywords: intrinsic security; system engineering; enterprise architecture; cybersecurity capability

1 数字化时代的网络安全体系需求演进

全球经济已全面进入数字化时代，中国在“十四五”规划中也明确提出了“加快数字化发展，建设数字中国”的战略规划。近年来，“网络强国”“加快培育数据要素市场”“加强数字政府建设”等一系列与数字化转型紧密相关的战略部署，都将数字化转型作为重要的发展战略与核心经济驱动力。数字化的核心不仅在于云计算、大数据、5G、物联网、人工智能、智能制造、卫星互联网这些新技术的应用，更在于将信息技术与政企机构业务运营、管理流程融合在一起，形成新的业务运营模式，从而显著提升业务运营效率和效益，为政企机构带来巨大的创新红利。与此同时，信息技术与业务的深度融合也将增加网络安全方面的风险，使得网络安全问题对业务产生破坏性乃至灾难性的影响。在这种情况下，网络安全风险将会等效于业务运营风险。政企机构信息系统一旦被入侵或被破坏，将会直接危害业务运营，进而危害生产安全、社会安全，甚至国家安全。这也是国家在数字化转型期从战略与法律法规角度，频繁推出《网络安全法》《数据安全法》《个人信息保护法》《网络安全等级保护制度》等一系列法律、法规、制度、标准的原因。

近年来，随着数字化环境的变化，网络空间威胁也发生了新的变化：各类新型的威胁如勒索攻击、大规模数据泄漏、供应链攻击、高级威胁高级持续性威胁（APT）攻击、内部威胁、国家网络空间对抗等相继出现，并带来了一系列影响。数字化转型对政企机构运营模式的转变是颠覆性的、不可逆转的，传统的信息化模式也将无法支撑目前经济环境下的业务运行要求。因此，政企机构必须立足于数字化业务运营的安全、高效、可靠运行，建设具有动态、综合、可持续等特点的适应于数字化业务的新型网络安全保障体系。

2 内生安全的理念

“内生安全”是指面向数字化业务，将网络安全能力内置到数字化环境中，并通过信息化系统和安全系统的聚合、业务数据和安全数据的聚合、IT人才和安全人才的聚合，让网络安全系统像人的免疫系统一样，实现自适应、自主和自成长，从体系化全局视角构建出动态综合的网络安全防御体系[1]。

从内生安全理念的产生到框架设计方法的形成与落地，相关实践指引了中国大量的大型政企机构的网络安全体系设计、建设、运行。这些实践与系统工程及企业架构（EA）方法论的结合与应用，起了关键作用。

系统工程产生于20世纪50年代，被广泛地用于航空、航天、机械制造、电子工程等各个领域，并由钱学森院士在中国积极倡导并开拓创新。系统工程是看待复杂系统（SoS）时的一种逻辑思维方法，是组织、管理“系统”规划、研究、设计、制造、试验和使用的科学方法[2]。系统工程专注于复杂系统的整体设计，从问题的全局视角来审视，为系统整体而非单一子系统设计方案，将所有变量都考虑在内，并梳理其相互关系。从系统化的视角来看，系统作为整体所产生的价值主要来自各组成部分的相互联系和相互作用关系，而且远远超过各组成部分的单独贡献的和[3]，这也就是所谓系统工程的“涌现”效果。

如果将日益复杂的数字化环境也视为一个复杂系统，那么EA就是系统工程在信息化领域的应用。在过去的20～30年，EA方法论在引导与推动大规模、体系化、高效整合的信息化建设、支撑各行各业科学地展开业务运营等方面都起到至关重要的作用，而内生安全框架亦有很多思路来源于EA方法论。通过创建、沟通、提高等方法，EA可以描述企业未来状态和发展的关键原则，进而把商业远景和战略转化成有效的企业变革。EA方法主要用于维护信息技术（IT）体系，或引入新的信息技术体系，从而实现组织的战略目标和信息资源管理目标。

1987年，J. ZACHMAN在《A Framework for Information Systems Architecture》中首次提出了“信息系统架构框架”的概念，从“信息、流程、网络、人员、时间、基本原理”6个视角来分析信息系统架构，由此奠定了EA的理论基础[4]。美国的一些机构率先使用EA：美国国家技术标准研究所（NIST）于1989年发布企业架构模型（NIST EA Model），于1999年发布联邦企业架构框架（FEAF），于2003年发布国防部体系架构框架（DoDAF）。同时，在企业机构和一些标准化组织中，也涌现出一些具有影响力的框架，例如开放标准组织体系结构框架（TOGAF）。

EA是企业业务战略与IT战略之间的接口，是企业顶层设计的图纸，决定企业结构、组成部分、各部功能、空间关系等元素。一般来说，EA可以分为两大部分：业务架构和IT架构。目前大部分EA方法都是从IT架构发展而来的。业务架构是把企业的业务战略转化为日常运作的渠道。业务战略决定业务架构，它包括业务的运营模式、流程体系、组织结构、地域分布等内容。而IT架构，是指导IT投资和设计决策的IT框架，是建立企业信息系统的综合蓝图，包括数据架构、应用架构和技术架构3部分。其中，业务架构的重点是流程和数据，而IT架构的重点是应用和技术。前者增加了企业愿景和任务目标驱动，后者增加了可落地的实施策略和计划。

作为系统工程思想在信息化领域的应用，EA方法打破了零散式的规划与建设，系统性地构建信息化体系，从而推动了大规模、体系化、高效整合的信息化建设。在很长一段时间里，网络安全在方法论上都缺乏这种体系化与全局视角。我们要做的就是从EA的方法体系与各种框架中，找到适合中国网络安全状况的方法，并结合具体国情，加以开发与利用，并结合内生安全理念，形成适用于网络安全的框架、方法与配套工具等。

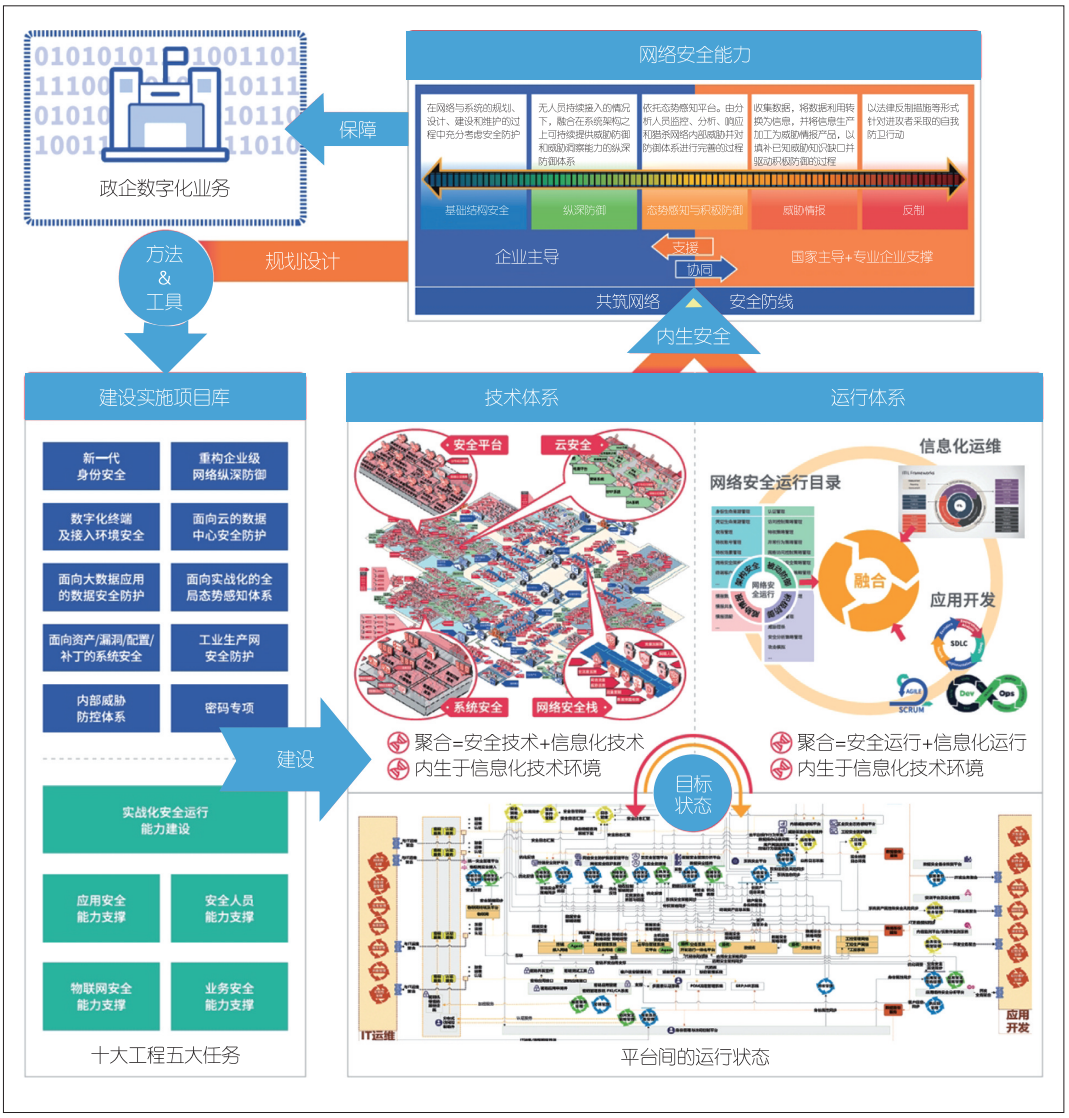
在网络空间安全领域对EA方法论的使用，是为了帮助政企大型机构理清并实现所需的“网络安全能力体系”，而不是为了建设某种具体的系统或产品。我们需要从全局视角了解大型政企机构所需的网络安全能力体系是什么？包含什么？应该如何有序地构建，并真正运行起来。我们要做的是进行合理恰当的选取与应用，从全局视角以系统性的方法进行整体的设计、建设与运行。我们应当综合考虑业务现状与信息化环境的未来发展，规划设计与之相匹配的网络安全能力体系，并像信息化的建设一样，将网络安全的能力与数字化融合内生，做到与信息化环境全面覆盖以及深度融合，从而保障政企核心业务的顺畅运行。

根据政企机构信息化与网络安全建设的实践经验，我们总结了一套适合于中国政企机构，特别是大中型政企机构信息化发展的、系统性的网络安全建设框架。新框架即是对网络安全模式升级新方法的探索，也是“内生安全”理念的有效落地。

3 内生安全框架与体系设计方法

借鉴EA方法论，以“网络安全能力体系”建设为中心，内生安全框架可以识别出在信息化的各个层面构成网络安全能力的能力组件，并将这些安全能力组件全面覆盖至政企普遍存在的信息化各领域，进而规划出网络安全建设实施“项目纲要库”（需要逐步实施的项目的集合）。随着这些项目的实施，安全防护体系将逐步融入信息化环境，进而共同实现全面的安全能力。最终，安全技术体系与安全运行体系的建立完善，可以实现“内生安全”的全面落地，并使政企机构能够具备体系化的安全防御能力。

内生安全框架（具体如图1所示）涉及的安全能力应全面覆盖云、终端、服务器、通信链路、网络设备、工控、人



▲图1 内生安全框架[1]

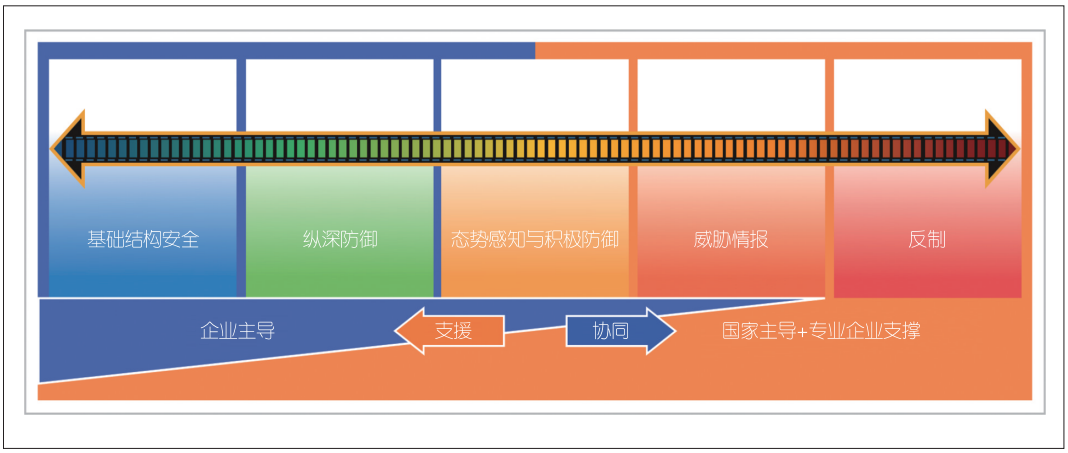
员等IT要素，避免因局部盲区而导致的防御体系失效；还需要将安全能力深度融入物理、网络、系统、应用、数据与用户等各个层次，确保安全能力能在IT的各层次有效集成。

内生安全框架为大型政企机构在数字化转型的快速发展期开展整体的网络安全规划与体系设计提供了思路与建议。我们通过该框架，从“甲方视角、信息化视角、网络安全顶层视角”展现出政企网络安全体系全景，通过以能力为导向的网络安全体系设计方法，规划出面向中长期的建设实施项目纲要库（即重点工程与任务，其进一步的扩展与细化可以形成网络安全相关重点领域的参考架构），并设计出将网络安全与信息化相融合的目标技术体系和目标运行体系，供政企机构参考、借鉴。

通过“叠加演进的能力分类方法”，内生安全框架形成面向政企信息化全领域的网络安全能力体系。政企可结合自身情况，采用框架中包含的方法工具，对每个安全领域的安全能力进行组合，重点设计能力间的逻辑关系以形成能力逻辑架构，并规划出覆盖网络安全领域的建设实施项目库。在规划周期内，项目库中的工程和任务依据路线图确定的时间开展研究、立项、建设。随着项目和任务的落地，政企将逐步建成目标技术体系架构与目标运行体系架构。体系化的网络安全能力也会随之达成，从而保障了数字化业务。

网络安全能力体系是保障政企机构数字化业务运营所必须的网络安全能力的集合。只有政企机构具备了这些必须的安全能力，才能真正有效地保障数字化业务安全。在框架的组成中，网络安全能力体系通过结合全球安全领域的规范标准、最佳实践、新安全技术，枚举出了保障政企机构数字化业务安全运行所需的能力集合。借鉴国际网络安全研究机构（SANS）提出的网络安全“滑动标尺”模型[5]，我们对安全能力进行分类，并结合中国政企机构信息化普遍存在的安全领域，规划、设计并形成了适合具有中国特色的“叠加演进”的网络安全能力体系。

如图2所示，网络安全能力体系包含五大类，即基础结构安全（Architecture）、纵深防御（Defense in Depth）、态势感知与积极防御（Active Defense）、威胁情报（Intelligence）和反制（Counter）。其中，基础结构安全、纵深防御、积极防御、威胁情报这4类能力是一个完备的政企业级网络空间安全防御体系所需的，而反制能力主要由国家级网络安全防御体系来提供。



▲图2 叠加演进的网络安全能力模式

• 基础结构安全：在系统规划、建设和维护的过程中，我们应该充分考虑安全要素，确保这些安全要素被设计到系统中，从而构建一个安全要素齐全的基础架构。

• 纵深防御：该能力体系是建立在架构安全基础上的，并能在多道网络防线上提供持续的威胁防御或威胁洞察力。该能力就像是给整个机构构建了战场防御的“纵深”，并在阵地的不同层次、不同区域上进行不同技术类型的层层设防，并保证其防御策略行之有效。

• 积极防御：在该能力体系中，主动防御、数据分析被充分利用，分析人员开始介入，形成人机互动，并对网络内的威胁进行监控、响应、学习和理解。积极防御把攻防过程从看似离散的告警，进化成一个有时空关联的完整过程；把攻击发生时的瞬间防御，变成了日常的监测、分析和学习的过程；把对单次攻击本身的检测，延伸到对攻击者和攻击者持续行为的关注。

• 威胁情报：该阶段的主要任务是收集和分析内部数据，并使用外部第三方威胁情报数据。更多来源的威胁情报的利用，能够使防御体系有更广泛的视角。这样能够综合了解行业、区域，甚至全球的网络攻击的现状、方法与相关攻击指标（IOC），从而通过可机读情报的处理过程来大大提升防御系统的告警准确性与效率。

• 反制：该能力指在友好网络之外，对攻击者采取直接的压制或打击行动。不过，按照中国网络安全法律、法规的要求，对于一般的政企机构来说，在进攻反制阶段所能做的，主要是通过法律手段对攻击者进行反击或借助国家力量进行网络安全监管。

从叠加演进的视角来看，网络安全防御能力体系中的基础结构安全与纵深防御能力具有与信息基础设施“深度结合、全面覆盖”的综合防御特点，而积极防御与威胁情报能力具有“掌握敌情、协同响应”的动态防御特点。这些能力间彼此关联、相互促进。

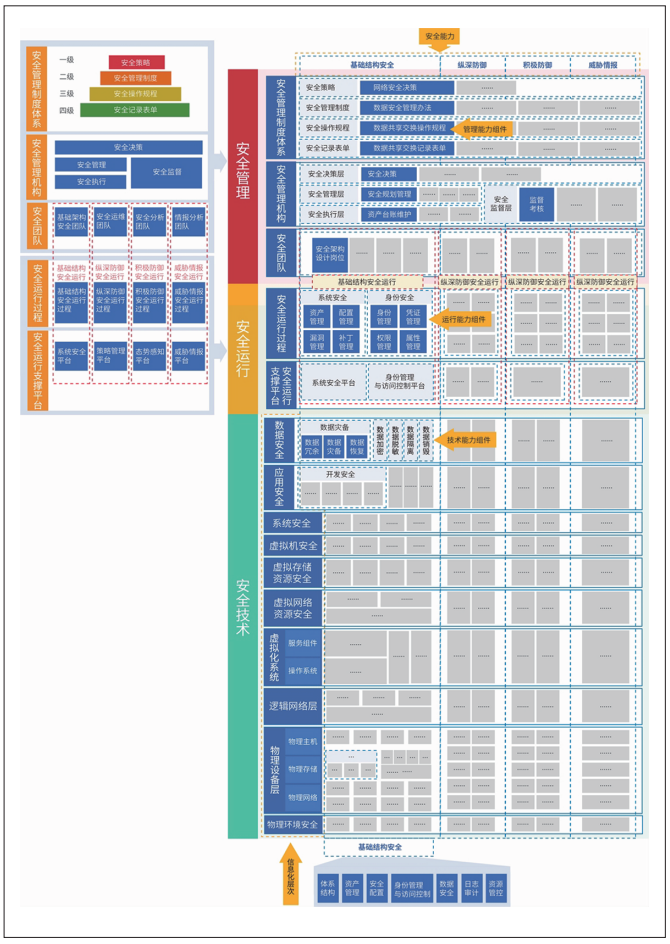
对于数字化的系统来说，IT与业务是密不可分的。从EA方法论出发，上述网络安全能力应当与信息化相融合，以保障业务安全、有序地发展。通过识别、设计构成网络安全防御体系的基础设施、平台、系统和工具集，围绕可持续的安全运行体系进行集成整合，可以构建出动态综合的网络安全防御体系。需要注意的是，我们要避免“以偏概全”的传统模式，以全覆盖、层次化的思路进行规划、设计。以网络的纵深防御体系为基础，进一步以数据确定防御重点，开展实战化安全运行，规划、建设动态综合的网络安全防御体系，以确保安全能力在IT的各层次有效内生。

通过组件化安全能力，内生安全框架将网络安全能力映射为可执行、可建设的网络安全能力组件，具体如图3所示。安全能力组件是安全能力的实现载体，具体包括安全管理、安全技术、安全运行相关内容。在政企机构信息化的所有层面，把安全能力组件与信息化组件相结合，保证了安全能力对信息化的覆盖与融合。通过对安全组件的组合，能够定义出要建设的项目，并清晰地表达项目的建设内容。

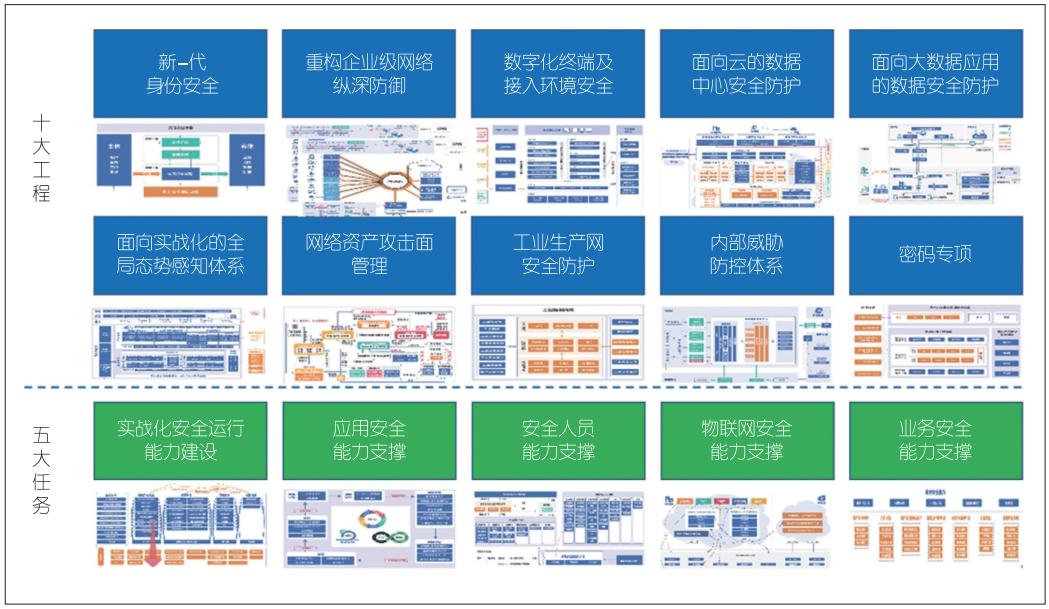
在政企机构网络安全的实际规划、设计、建设、运行、落地的过程中，项目是推行安全管理思想、强化安全管控、提升安全能力的重要抓手。在安全规划中，项目设置的科学性、合理性、可落地性是决定安全体系建设成效的关键因素。通过使用基于“能力导向”的EA方法论，内生安全框架将政企的网络安全防御体系作为一个整体复杂系统进行设计，并在此过程中识别出了15个“构成子系统”，即“十大工程、五大任务”，具体如图4所示。进一步地，内生安全框架以系统工程的方式将这15个构成子系统分别作为“复杂系统”进行设计，从而梳理清晰其全景与相互依赖关系。

在框架的工具集中，我们面向这15个子系统设计了项目规划纲要。项目规划纲要是项目库的核心。从项目建设与实施的视角出发，项目规划纲要高度概括了项目的目标、覆盖范围、预期效果、协同领域以及多个项目之间的作用关系，强调项目规划、可研、立项与设计阶段的关键要点。

政企机构在网络安全规划时可参考项目规划纲要模板，



▲图3 组件化安全能力



▲图4 项目实施纲要库

并根据政企现状规划项目，向信息化领导和网络安全领导阐述项目的重要意义、必要性、建设内容等，以得到充分的资源配给和政策支持。在规划的全周期内，政企参考项目规划纲要进行可研、立项、招标、初步设计、概要设计、建设和运行，明确项目执行中每个系统须达到的预期能力、关键指标和协同关系，确保安全能力的完整性、体系性和可落地性，进而以一个可实现、一贯秉承的整体视角持续建设，以达成网络安全防御目标。

4 内生安全“构成系统”的技术要点与参考架构

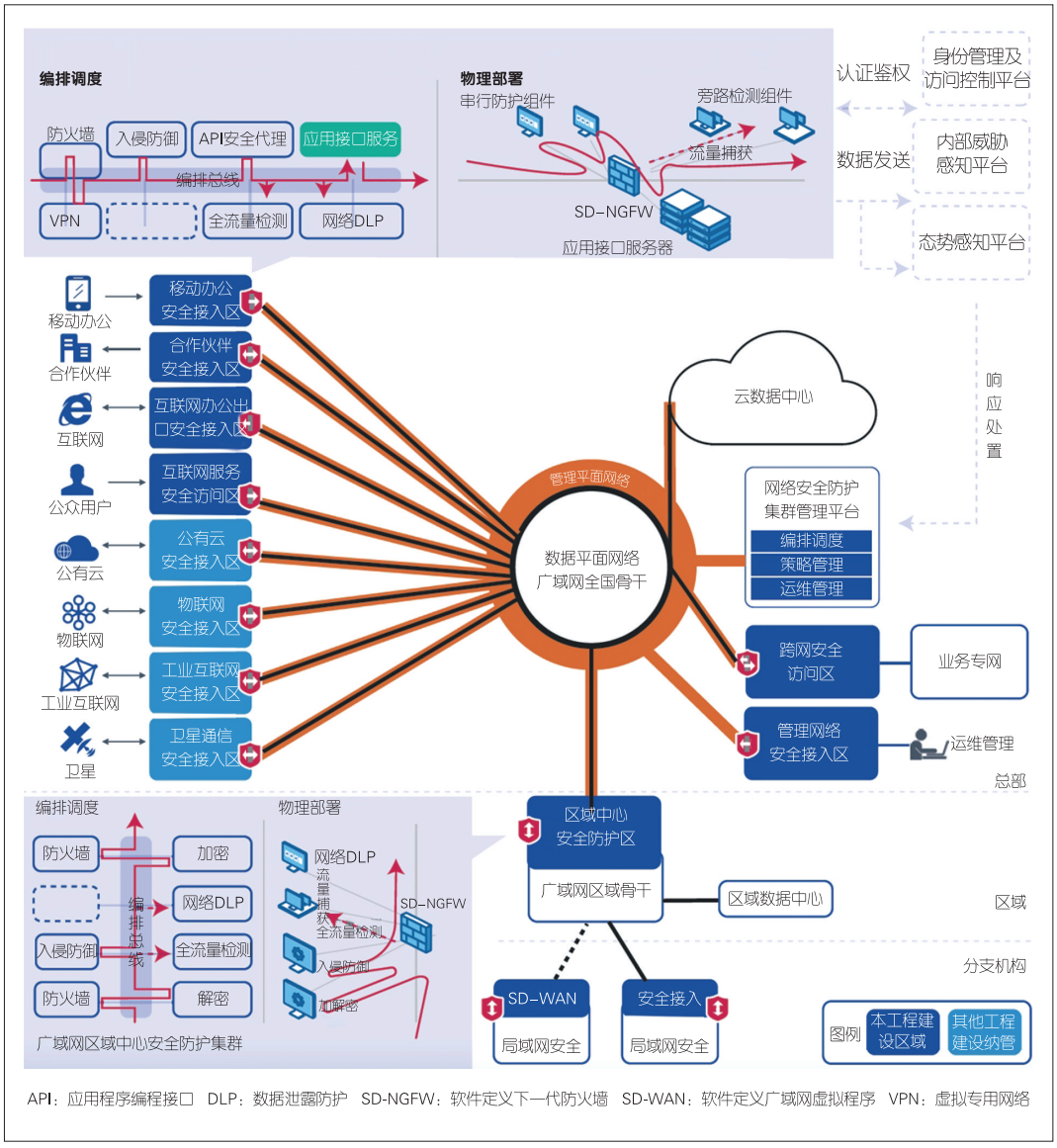
在内生安全框架的每一个项目纲要库中，通过进一步的扩展，能够间接起到构建该领域的“参考架构”的作用。“参考架构”一般不会具体明确实现该领域能力体系的具体方案或服务细节，而是会从该领域（子系统）的能力体系出发，给出子系统网络安全的能力要求与技术要点。而具体采用何种落地方案、产品、服务，则不受限制。这样也能够在保证网络安全防御目标达成的同时，采用多样的技术路线来灵活实现。下面，我们从两个角度进行说明：最基础的网络纵深防御和目前最受关注的数据安全。

网络纵深防御是网络安全体系中最基础的子系统，其整体架构如图5所示。在数字化转型进一步升级、网络变得越来越开放与复杂的情况下，网络纵深防御已不再是简单的边界防护，而是有了更多的具体要求。在这种挑战下，“重构企业级网络纵深防御”工程给出了设计的参考架构与样例库。

从设计原则上，该工程给出了“最小攻击面设计”“面向失效的设计”“能力导向的设计”3个原则。在总体架构上，通过在大型政企网络中构建多级网络纵深，并在纵深与各安全域上进行威胁模型分析，建立纵深防御策略矩阵。

网络纵深防御最终遵循8个方面的技术建设要点，具体包括：

（1）设计标准化、模块化的各类网络安全防护集群，提供流量清洗、网络访问控制、加/解密、入侵防范、恶意代码防范、应用安全防护、安全代理、数据泄漏检测、全流量检测、攻击诱捕等安全能力，通过软件定义



API：应用程序编程接口　DLP：数据泄露防护　SD-NGFW：软件定义下一代防火墙　SD-WAN：软件定义广域网虚拟程序　VPN：虚拟专用网络

▲图5 网络纵深防御整体架构

网络等技术实现安全能力服务化、弹性扩展和灵活调度编排，适配各节点的安全防护需求。

（2）规整网络外部边界，收敛应用服务及接口的协议类型，分别部署网络安全防护集群：建设合作伙伴安全接入区，保障对外接口及数据安全；建设互联网安全接入区，保障互联网服务访问安全；建设互联网办公出口安全接入区，保障用户上网行为安全；纳管其他工程建设的公有云安全接入点、物联网安全接入区、工业互联网安全接入区、卫星通信安全接入区。

（3）在业务专网、涉密网等不同密级的网络间集中建设跨网安全访问区，部署网络安全防护集群，提供网络访问控制、应用程序编程接口（API）安全代理、数据隔离与交换等能力，确保用户跨网访问及数据交换的安全。

（4）在广域网各区域中心节点建设区域中心安全防护区，部署网络安全防护集群，以增加广域网安全防护纵深，形成多层次、协同联动的广域网纵深防御能力，全面缩小广域网暴露面，从而降低横向移动的可能性。

（5）在广域网各分支节点建设分支机构安全接入点，通过软件定义广域网（SD-WAN）技术，实现网络访问控制、传输加密、入侵防范等能力，保障大量分支机构节点的安全接入，优化广域网线路成本，提高部署和运维工作效率。

（6）建设独立的管理网络，以实现数据平面与管理平面分离，收敛硬件管理接口，从而确保运维管理通道资源的可用性。建设、管理网络安全接入区，部署网络安全防护集群，基于零信任架构和基于属性的访问控制模型，与身份管理及访问控制平台对接，实现运维特权账号管理，从而对运维管理操作实施动态细粒度访问控制，最小化对资源的访问权限。

（7）将各安全防护集群的安全数据接入安全运行与态势感知平台，为安全分析提供全局网络安全数据支撑。

（8）面向各节点的网络安全防护集群，建设统一的运行管理平台，以实现安全策略全生命周期自动化管理，从而支撑态势感知平台安全事件的响应处置。

根据具体的网络环境场景，上述建设要点完整地呈现了系统架构中的组件要素及它们相互之间的逻辑关系，能够帮助政企机构在该领域形成更准确的项目定义，而不仅仅是简单的产品堆砌。因此我们需要瞄准一个可实现、有依据的目

标，进行全景设计。对于这其中所涉及到的技术要点，我们并不会强制地规定具体的实现方式，而是更为关注其所需要的安全能力，以及实现这些能力所必要的组件、子系统、模块，以及它们之间的逻辑关系和集成关系。这些内容的进一步细化与扩展，就能够起到“参考架构”的作用。

另外一个例子是数据安全。与最为基础的网络纵深防御相比，数据安全领域则更加能够体现了“内生”的重要性。为了描述得更清晰，我们会用到系统工程中的一个工具ConOps，具体如图6所示。

数据安全运行构想图共有4层：

（1）数据安全策略层。该层的重点是健全数据安全管理制度，能根据数据安全治理的结果，构建相应的数据安全策略，从而帮助机构明确数据安全所需的组织、规范、制度、流程等。从业务场景、应用逻辑出发，基于数据安全治理阶段的成果（数据脉络、数据标签、数据分类分级等）构建需要基于属性的数据安全策略，以向下面的3层进行分发。这一层更多的是与数据安全的管理相关。

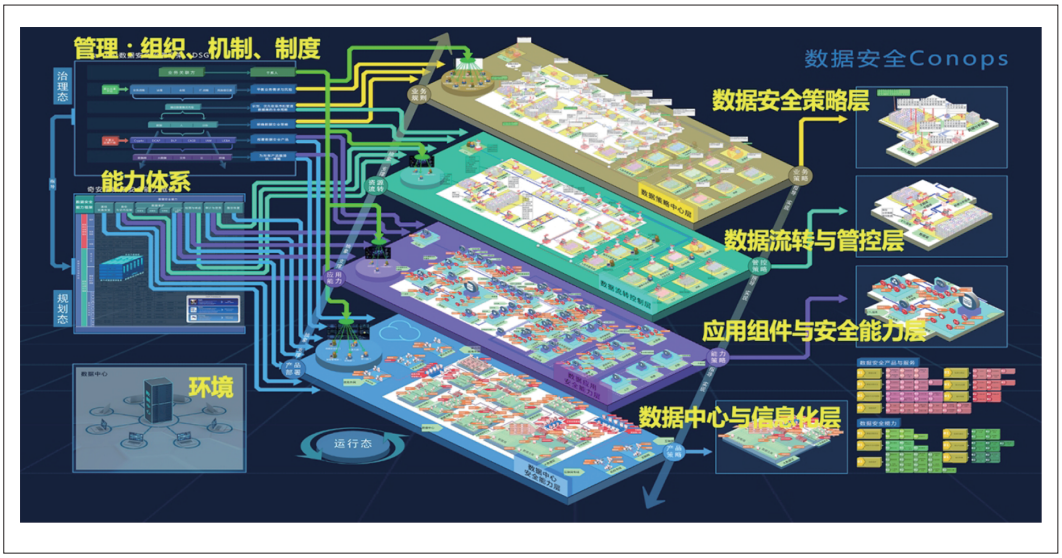
（2）数据流转与管控层。该层的重点是确保数据的流转有序合规、数据使用的行为规范，并实现对数据的全面梳理和有效防护。在这一层中，我们要全面梳理数据资产，确定适当的数据安全等级，并设定多样化的属性标签，从而全方位描述与数据安全管控可能相关的数据信息；通过明确管控数据的流转，并结合数据流转监测，发现非法用户窃取数据等异常行为；根据数据流转与管控策略，以“权限最小化”原则进行授信。未来，我们可通过零信任体系进行动态评估，从而实现对数据的动态、细粒度访问控制；对数据使用行为留痕，从而为实时的监测响应和审计提供支撑。

（3）应用组件和安全能力层。该层用于描述新型数据中心中业务应用的运行态，并基于业务系统的逻辑和应用架构，将各个应用组件和各组件之间的逻辑关系呈现出来，同时将每个组件和应用所需要的安全能力嵌入到组件中，从而将安全能力与应用内生融合。进一步地，根据数据安全治理的成果做相关的安全保护（如加密、脱敏、去标识化等）。同时，应用安全策略的落地会集中在这一层，“身份与访问控制、信息保护、监测与响应、审计与定责”为之提供能力支撑。

（4）数据中心和信息化层。该层的重点是保障数据的载体和业务运行环境的安全，包括数据中心安全区域划分、边界网络安全栈防护、服务器加固、系统与资产安全的保障等。该层是数据的载体和业务运行的基础环境，是数据安全的基础保障。

数据中心安全能力层是以体系化的方式，保障数据运行环境的安全。数据中心安全区域的划分，保证了不同安全等级业务在适合的区域运行，以及不同安全等级数据的有效隔离；数据中心网络安全栈防护，是为了做好边界安全的防护抵御外部攻击；服务器加固与防护，是对应用和中间件进行持续监控保护，防止服务器遭受APT和0DAY攻击；而面向资产、配置、漏洞、补丁的系统安全，可以解决资产不清、配置不明、漏洞分布不知、补丁修复缓慢等问题。

我们可以看到，在数据安全运行构想图中，各层级之间可以实现有效连接和运转。自上而下看，这是策略的逐层实现与落地；自下而上看，这是从产品部署到应用能力，再到业务流转及逻辑规则的支撑与提炼。尤其是最上面的两层，说明了与传统的网络安全相比较，要想做好完整的数据安全保障，一定会介入数据流转、应用逻辑、管理策略，这就更加体现了“内生”的思想。在数字化时代的新应用与数据安全体系中，安全能力不仅仅要内生于信息化环境，甚至要内生于应用与业务逻辑，以及数据流转与管理策略当中。



▲图6 数据安全ConOps运行构想图

5 结束语

迄今为止，内生安全框架在近3年已经被应用

下转第56页➡

Autonomic and Secure Computing. IEEE, 2006: 227–234. DOI: 10.1109/DASC.2006.24
[12] 邬江兴. 网络空间拟态安全防御 [J]. 保密科学技术, 2014(10): 4–9+1
[13] 邬江兴. 网络空间拟态防御研究 [J]. 信息安全学报, 2016, 1(4): 1–10. DOI: 10.19363/j.cnki.cn10–1380/tn.2016.04.001
[14] 丁绍虎, 李军飞, 季新生. 基于拟态防御的SDN控制层安全机制研究 [J]. 信息安全学报, 2019, 4(4): 84–93. DOI: 10.19363/J. cnki. cn10–1380/tn.2019.07.06
[15] 仝青, 张铮, 张为华, 等. 拟态防御Web服务器设计与实现 [J]. 软件学报, 2017, 28(4): 883–897. DOI: 10.13328/j.cnki.jos.005192
[16] 张铮, 马博林, 邬江兴. web服务器拟态防御原理验证系统测试与分析 [J]. 信息安全学报, 2017, 2(1): 13–28. DOI: 10.19363/j. cnki. cn10–1380/tn.2017.01.002
[17] 任权, 贺磊, 邬江兴. 基于离散马尔可夫链的不同抗干扰系统模型分析 [J]. 网络与信息安全学报, 2018, 4(4): 30–37. DOI: 10.11959/j. issn. 2096–109x.2018035
[18] DAI W B, LI S Y, LU L, et al. Research on application of mimic defense in industrial control system security [C]//Proceedings of 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA). IEEE, 2022: 573–577. DOI: 10.1109/ICIBA52610.2021.9688212
[19] KIM J, BENTLEY P J. Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection [C]// Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600). IEEE, 2002: 1015–1020. DOI: 10.1109/CEC.2002.1004382
[20] KIM J, BENTLEY P. Immune memory and gene library evolution in the dynamic clonal selection algorithm [J]. Genetic programming and evolvable machines, 2004, 5(4): 361–391. DOI: 10.1023/B: GENP.0000036019.81454.41
[21] NESPOLI P, MÁRMOL F G, VIDAL J M. A bio–inspired reaction against cyberattacks: AIS–powered optimal countermeasures selection [J]. IEEE access, 2021, 9: 60971–60996. DOI: 10.1109/ACCESS.2021.3074021
[22] 罗娅, 陈文. 一种基于核熵和人工免疫的网络异常检测方法 [J]. 西南师范大学学报(自然科学版), 2016, 41(6): 119–124. DOI: 10.13718/j. cnki.xsxb.2016.06.019
[23] YU Q, REN J, ZHANG J Y, et al. An immunology–inspired network security architecture [J]. IEEE wireless communications, 2020, 27(5): 168–173. DOI: 10.1109/MWC.001.2000046

作 者 简 介

胡爱群，东南大学网络空间安全学院教授；主要研究领域为信息系统安全、物理层安全、内生安全等；主持和参与国家“863”计划、国家自然科学基金、国家支撑计划、国家发展改革委信息安全专项、企业合作项目数十项；发表学术论文100余篇，获授权国家发明专利40余项。

李涛，东南大学网络空间安全学院副教授；主要研究领域为信息系统安全、内生安全、智能安全。

卞青原，东南大学网络空间安全学院在读硕士研究生；主要研究方向为内生安全。

➡上接第35页

在超过百家的大型政企机构的“十四五”网络安全规划、3—5年中长期网络安全规划设计、重点领域的网络安全专项设计与建设当中，包括大型部委、能源央企、制造业央企、大型民营智能制造企业、银行与金融机构、数字城市等的数字化新型网络安全体系的构建。

在2022年北京冬奥会的网络安全保障工作中，内生安全也发挥了重要作用。人们基于内生安全框架，系统性、全局性地设计了冬奥会网络安全保障体系，统筹部署了整体安全运行工作。通过基于内生安全的“联合作战、精准防护、深度运营”，在冬奥会期间，分析日志的数据总量超过1 850亿条，修复中高危漏洞5 800余个，累计监测网络攻击尝试超3.8亿次，跟踪、研判、处置重点网络安全事件105件，最终实现了奥运网络安全保障历史上第一次“零事故”的成果。

未来内生安全的理念、框架，以及配套的能力体系模型、工具、参考架构、纲要库等，也会继续为中国重要政企机构网络安全保障、关键信息基础设施保护、重大活动网络安全保障贡献更多的力量。

参考文献

[1] 奇安信战略咨询规划部. 内生安全 新一代网络安全框架体系与实践 [M]. 北京: 人民邮电出版社, 2021
[2] 钱学森. 论系统工程 [M]. 长沙: 湖南科学技术出版社, 1982
[3] 朱一凡. NASA系统工程手册 [M]. 北京: 电子工业出版社, 2012
[4] ZACHMAN J A. A framework for information systems architecture [J]. IBM systems journal, 26(3): 276–292. DOI: 10.1147/sj.263.0276
[5] LEE M R. The sliding scale of cyber security [R]. SANS Institute, 2015

作 者 简 介

韩永刚，奇安信科技集团副总裁、战略咨询规划业务负责人，中国计算机学会计算机安全专业委员会委员、中国计算机行业协会数据安全专业委员会数据安全产业专家委委员；有近20年的网络安全领域经验，专注于数字化转型中的新一代网络安全体系规划设计与构建、内生安全体系、态势感知与大数据安全分析、数据安全、城市安全运营等方向；曾带领团队开展中石化“十四五”网络安全规划，南方电网“十四五”网络安全规划，中国人民银行业务网网络安全三年规划等多个大型部委、央企、数字城市的网络安全规划与体系设计。