5G智慧城市泛在安全防护探讨

Discussion on Ubiquitous Security Protection of 5G Smart City

刘　毅[1]，于　乐[1]，张　峰[1]，马禹昇[1]，林艳纯[2]（1. 中国移动通信集团有限公司，北京 100053；2. 中国移动通信广东公司，广东 广州 510000）

Liu Yi[1]，Yu Le[1]，Zhang Feng[1]，Ma Yusheng[1]，Lin Yanchun[2]（1. China Mobile Communications Group Co.，Ltd.，Beijing 100053，China；2. China Mobile Communications Guangdong Branch，Guangzhou 510000，China）

摘　要：

随着“新基建”战略的发布与推进，在5G、算力网络等新技术新应用的推动下，智慧城市已进入规模化建设阶段，同时也伴随着安全威胁的持续变化。国家针对安全可控、网络安全、智慧城市建设作出重要指示，在十四五规划中也提出要建设智慧城市和数字乡村、要加强网络安全保护、建立健全数据要素市场规则。在5G、算力网络、智慧能力建设的基础上，提出了高速、移动、安全、泛在的“连接能力服务”，构建“一点接入、即取即用”的“新型算力服务”，该方案已在某市的业务系统中应用部署，取得了良好的应用效果。

关键词：

智慧城市；算力网络；云网安全能力；连接

doi：10.12045/j.issn.1007-3043.2022.09.007

文章编号：1007-3043（2022）09-0027-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the release and promotion of "new infrastructure" strategy，smart cities have entered the stage of large-scale construction driven by new technologies and applications such as 5G and computing power network，and security threats continue to change. The government has given important instructions on safe and controllable，network security and the construction of smart cities. In the 14th Five-Year Plan，it also states that smart cities and digital villages should be built，network security protection should be strengthened，and market rules of data elements should be established and improved. On the basis of 5G，computing power network and smart capability building，it proposes high-speed，mobile，secure and ubiquitous "connectivity services"，which is a "new computing force power service" that can be "connected at one point，ready to use". The scheme has been implemented in a city and has achieved good application results.

Keywords：

Smart city；Computing power network；Cloud network security capability；Connection

引用格式：刘毅，于乐，张峰，等. 5G智慧城市泛在安全防护探讨[J]. 邮电设计技术，2022(9)：27-31.

1 5G智慧城市安全概况

1.1 建设背景

近年来，国家针对数字中国、智慧社会、基础设施建设等提出了战略部署。国家重点提出要“加快建设创新型国家”、“为建设科技强国、质量强国、航天强国、网络强国、交通强国、数字中国、智慧社会提供有力支撑”，同时在未来深化改革的道路上，要“不断推进国家治理体系和治理能力现代化”[1]。

收稿日期：2022-07-11

依据规划，各地在持续推进政务云建设，政务云在提升城市治理能力的同时，也带来新的安全风险。在城市政务应用的端、边、管、云多个不同层面，需要部署相应的安全能力来应对这些风险，亟需一套融合端到云的一体化安全解决方案。本文提出一种实现连接、算力到能力的云网安一体化防护体系，构建端到端安全管控服务，能够提升网络信息整体安全[2-3]。

1.2 建设内容

按照“集约高效、共享开放、安全可靠、按需服务”的原则，以“云网合一、云数联动”为构架思路，建立面向政务外网、政务云提供适应业务发展的动态安全防

护体系，持续安全运营，实现全域网络安全事前的攻击预测与风险管理，事中的监控预警、安全分析、关联分析以及事后的取证、溯源、修复达到安全防御闭环的同时，输出密码资源池、零信任访问管控、Web全栈防护、安全大数据建模等安全能力。

依据《电子政务外网安全建设规范》、《5G多接入边缘计算平台通用安全防护要求》等规范要求，从安全技术、安全运营管理、安全运维等3个方面开展安全防护建设。综合考虑系统平台物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的国密系统平台应用方案；通过Web全栈防护能力，使用“可编程、虚拟化”等技术实现了防御需求场景化，同时采用“安全资源池架构”解决应用层防御访问时延问题，在对抗过程中快速高效地实现安全防御；集合了相关数据资源，助力行业客户完善风险防控手段，提高精细化运营能力。

2 5G智慧城市安全框架

2.1 安全总体架构

如图1所示，基于“连接+算力+能力”的基础架构，以构建统一的“大安全”为基本思路，通过集中建设漏洞扫描系统、DDos防御系统、APT威胁检测系统、安全审计系统、堡垒机设施、安全数据采分平台、云加密设施、身份管理平台等基础设施，形成智慧城市安全大脑，实现安全统一管理和设施共享能力，打造运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、安全可闭环的政务云安全技术体系。

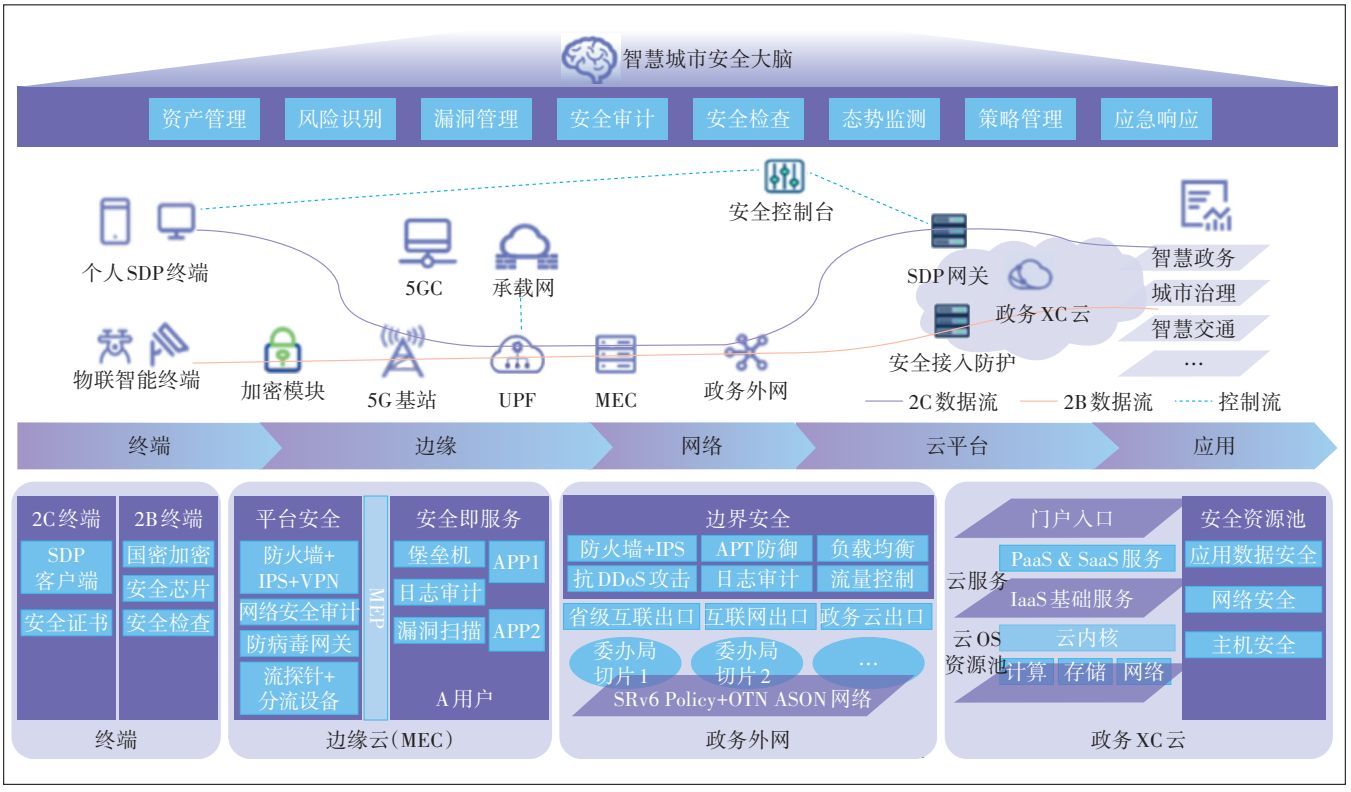

图1　智慧城市安全大脑

2.2 5G安全连接架构

多网融合的有线政务网络是以政务外网全新升级迭代为抓手，通过应用先进的OTN（Optical Transport Network）光传送网络，实现市、镇、村3级政务网络和全市党政部门纵横全面覆盖，实现了速度和覆盖面的10倍提升；通过SRv6（Segment Routing IPv6）等技术为多个政务专网整合划分单独虚拟专网承载，未来连接城市万路高清视频，数十万级物联终端及传感器。

泛在安全的5G政务专网（见图2）是在实现对政务单位全光纤接入覆盖的基础上，建设5G政务专网，实现业务隔离，保障政务专网安全，利用5G网络的广域覆盖与深度覆盖，实现灵活组网结构，实现固移融合、无线延伸，全方位支撑多网络、多场景、多领域的场景融合，为“万物互联”保驾护航。

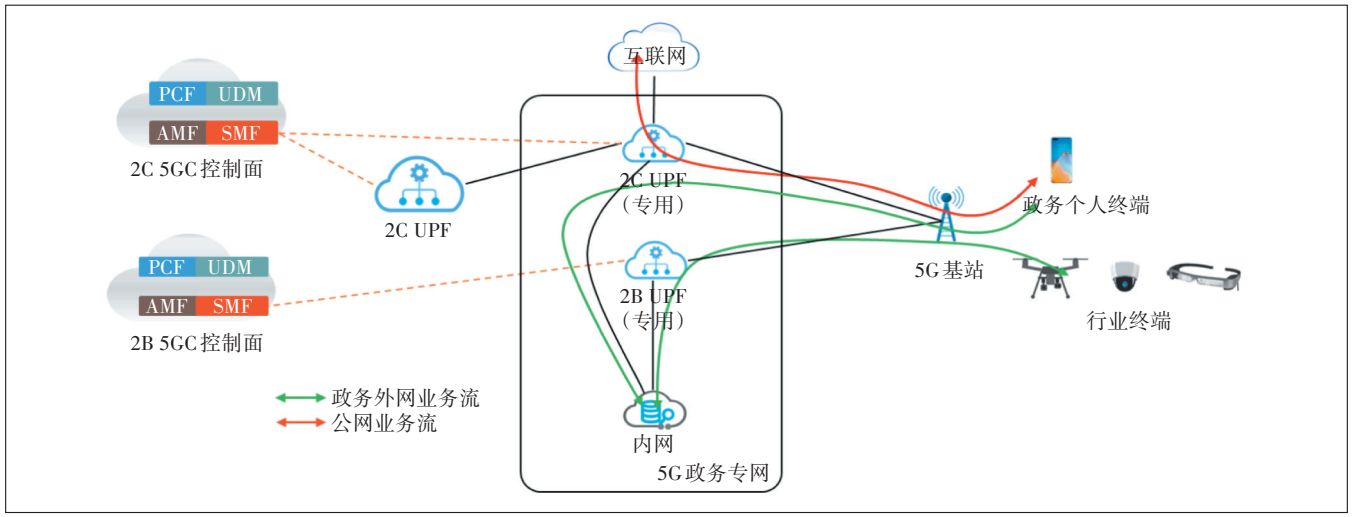

图2　5G政务专网

针对政务个人用户，建设专属的2C 5G专网，根据需要建设下沉2C UPF，满足客户不换卡、不换号，只需换手机的需求；针对行业应用终端，建设专属的2B 5G专网，建设下沉2B UPF，基于全市的5G基站，可满足视频采集、移动执法、视频监控、业务办理一体机等各种行业终端随时随地接入，方便行业终端的应用部署。主要的安全防护手段有：

a）设备可信：主要包括确保硬件安全、系统可信保障和设备接口保护。硬件安全包括从硬件接口的安全防护、防近端攻击到独立硬件安全模块等多个层次的保障；系统可信保障提供基于硬件信任根的系统或软件的静态可信验证，应用程序执行环境的动态可信验证，以及关键文件的机密性和完整性保护。

b）网络隔离：通过5G DNN实现端到端网络切片，实现网络隔离，重要网络区域与其他网络区域之间采取可靠的技术隔离手段，特别的，基于共享基础设施多制式、多业务网络共部署场景下通过技术隔离手段防御跨制式、跨业务网络攻击能力，最高支持物理隔离。

c）通信安全：采用5G设备终端密码技术进行机密性、完整性验证升级，保障无线接口和传输网络通信安全，可在高安全要求场景下支持基于硬件密码模块对重要通信过程进行密码运算和密钥管理。

d）终端安全防护：政务应用服务具有大量的各类终端感知设备，包括2C终端如5G智能手机、电脑等，海量的终端提供多维度的采集信息。针对2B场景，终端侧集成安全芯片或安全TF卡，或外接安全接入模块，实现SM1、SM2、SM3、SM4等国密算法支持[4-6]，提供高速数字签名/验证、非对称/对称加解密、数据完整性校验，保证敏感数据的机密性、真实性、完整性和抗抵赖性。

2.3 信创云架构

通过统一的信创云基础设施资源池，基于国产化芯片、操作系统、数据库等，结合现有的信息网络平台、网络安全防护、网络管理体系，应用虚拟化技术实现网络高可靠、架构弹性扩缩、资源利用率高且满足国家信创需求的统一基础设施资源池。

a）统一的信创云基础设施资源池：基于国产化芯片、操作系统、数据库等，应用虚拟化技术实现网络高可靠、架构弹性扩缩、资源利用率高且满足国家信创需求的统一基础设施资源池。

b）统一的信创云管理运营运维支撑平台：制定服务标准和规范，提供满足需求、响应及时、安全可靠的运维保障服务，建立统一的运营运维服务体系。

c）面向现代化云数据中心的安全体系：面向云服务交付层、云基础平台层的资源访问服务与资源运维管理活动，提供网络纵深防御、系统安全支撑、云特权访问控制、安全态势感知等数据中心级安全能力，构建统一支撑、管理及运营的云安全防护体系。

3 5G智慧城市安全防护能力

5G智慧城市安全防护能力是由一系列的安全能力共同打造，主要包括云网安协同联动、密码资源池、零信任访问管控、Web全栈防护和大数据建模能力等。云网安协同联动是在云网一体的基础上，考虑安全协同联动管控，能够提升云网一体化后的安全防护

水平;密码资源池可提供密码服务一体化的统筹管理模式,提升密码应用水平;Web全栈防护将安全产品真正整合成统一的防御架构,可实现对应用全生命周期的自动化持续监控与响应。

3.1 云网安协同联动

在云网融合一体的架构上,充分考虑了云网的安全协同联动管控。依靠安全管理控制系统,提供安全业务编排和策略统一管理。通过安全管理控制系统联动态势感知分析平台实现威胁检测结果转化为安全策略,并将安全策略下发到安全设备,实现安全设备的联动处置。

安全运营中心在纳管网络边界防护的基础上,通过对接云安全能力管理平台,纳管政务云的安全防护能力,实现云网的统一安全管控、统一安全监测、统一安全防护。

3.2 密码资源池

在政务云模式下,传统的网络边界变得模糊以及云计算带来的很多不确定因素,对安全技术提出了更高的要求。考虑到建设项目中已经规划的安全设施、软件、服务和产品,将密码应用建设统筹至整体安全建设中,与信息系统同步规划、同步建设和同步实施。通过健全网络和信息系统网络安全保障体系,完善密码基础设施,提升密码适用管理水平,推进密码在重要领域系统身份认证、安全隔离、信息加密、信息数据保护等方面的应用。

部署国密资源池后,应用国密改造可以只调用该国密资源池的资源,无需重新建设相关ssl vpn网关、密码机等资源。国密应用改造主要在网络通信及应用数据层进行,在网络通信链路上设计密码保护措施,能够保护用户、访问控制信息、安全标记、重要数据、关键操作行为等信息[11]。

3.3 零信任访问管控

通过建设统一的政务云平台,将各委办局应用系统进行集中纳管,统一维护管控仍然存在终端安全可信问题、应用对外服务暴露面大、基础身份用户信息不统一、信息孤岛等问题。“零信任”将网络防御的边界缩小到单个或更小的资源组,不自动信任内部或外部的任何人/事/物、不根据物理或网络位置对系统授予完全可信的权限,在授权前对任何试图接入政务系统的人/事/物进行验证,对数据资源的访问权只有当资源需要的时候才授予[12-13],如图3所示。

3.4 Web全栈防护

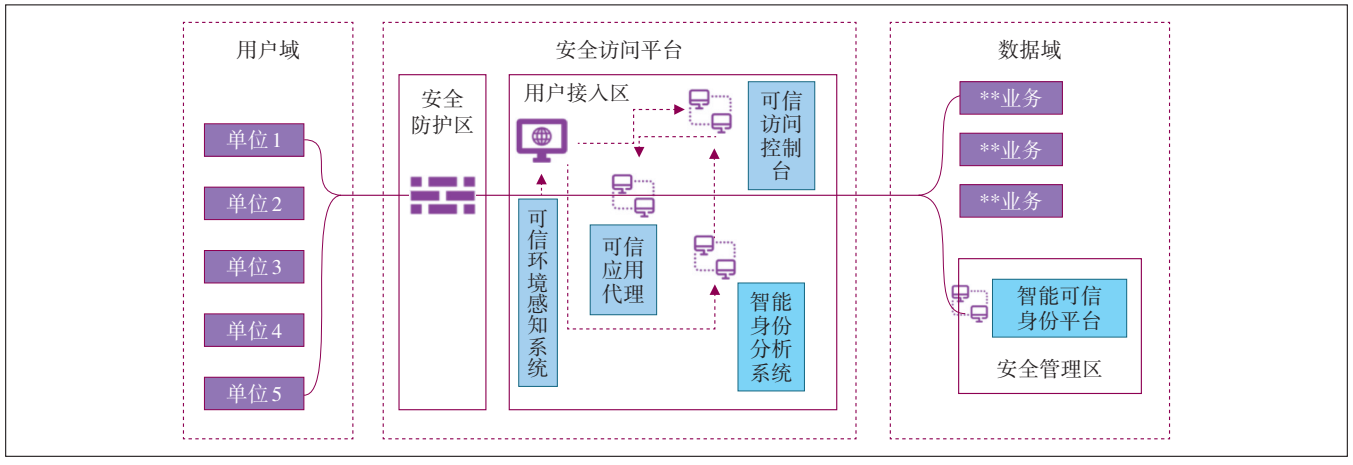

图3 零信任身份安全架构

Web全栈防护打破传统的安全防御思路,将安全产品真正整合成统一的防御架构避免各自为战,以国内外先进的可编程安全工具为基础,形成新一代网络安全产品,通过重新编辑将安全产品功能抽离,形成可定制的防御模板,通过“智能化、自动化、模块化”的基于脚本对抗的可编程防御架构,实现对应用全生命周期的自动化持续监控与响应(如图4所示)。

3.5 大数据建模能力

基于运营商海量用户业务数据,在政府和公共服务、国防安全、交通、医疗、金融等行业面向客户提供标准化数据标签,可应用于风险管控、精准营销等业务领域,助力行业客户完善风险防控手段,提高精细化运营能力[14-15]。政务云系统通过集成运营商亿级多维度的大数据能力,将运营商数据与自有市政、各金融用户维度数据相融合,结合安全多方计算、联邦学习、机密计算等技术为政务云用户输出安全大数据方

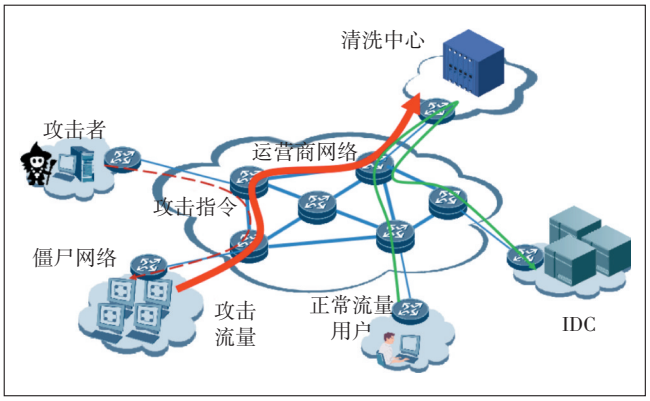

图4　全栈防护

案。

4 5G智慧城市建设实例

在某市政数局以“连接+算力+能力”为构建思路，构建了政务外网+政务云+安全能力输出的云网安一体化能力。在连接方面实现了5G+OTN的双引擎网络，提供以业务为维度的切片隔离，保障专网数据安全；在算力方面实现了统一管理的政务云的落地，实现云网安全协同联动；在能力方面，可以提供密码资源池、零信任访问管控、Web全栈防护、安全大数据建模能力等安全能力，输出统一封装、灵活调用的“云网安能力服务”。

目前项目已经落地，结合其电子政务外网服务项目实际情况，构建了电子政务外网服务项目的安全运营体系，形成威胁预测、威胁防护、持续检测、响应处置的闭环安全工作流程，打造四位一体的安全运营机制。建成以来日均发现疑似攻击1万余次，高风险安全事件4.6次，其中外网高危攻击1.3次，结合系统决策辅助与专家分析研判，均成功处置封禁，确保重大活动举办期间系统安全平稳运行。

5 总结

本文提出了一种5G智慧城市泛在安全防护方案，该方案基于“连接+算力+能力”的基础架构，以构建统一的“大安全”为基本思路，打造了运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、安全可闭环的5G智慧城市安全防护能力体系。该能力体系包含云网安协同联动、密码资源池、零信任访问管控、Web全栈防护和大数据建模能力等。未来，我们将在算力网络、数字孪生网络等方向进行深入研究，并提出适应客户业务发展的安全解决方案。

参考文献：

[1] 新华社.“十四五”规划和2035远景目标的发展环境、指导方针和主要目标[EB/OL].[2022-05-20]. http://www.gov.cn/xinwen/2021-03/05/content_5590610.htm.

[2] 向远金.政务云安全的一种解决方案[J].网络安全和信息化，2020(4):126-130.

[3] 陈亚男，李晨旸，刘海峰，等.一种基于密码云的政务云密码应用研究[J].信息安全研究，2020，6(9):844-848.

[4] ISO/IEC. IT security techniques — hash-functions — part 3: DEDICATED HASH-FUNCTions: ISO/IEC 10118-3: 2018[S/OL].[2022-05-20]. https://www.iso.org/standard/67116.html.

[5] ISO/IEC. IT Security techniques — digital signatures with appendix — part 3: discrete logarithm based mechanisms: ISO/IEC 14888-3: 2018[S/OL].[2022-05-20]. https://www.iso.org/standard/76382.html.

[6] ISO/IEC. Information technology — security techniques — encryption algorithms — part 3: block ciphers — amendment 1: SM4: ISO/IEC 18033-3: 2010/AMD 1: 2021[S/OL].[2022-05-20]. https://www.iso.org/standard/81564.html.

[7] 国家市场监督管理总局，国家标准化管理委员会.信息安全技术网络安全等级保护基本要求：GB/T 22239-2019[S].北京：中国标准出版社，2019.

[8] 国家市场监督管理总局，国家标准化管理委员会.信息安全技术网络安全等级保护安全设计技术要求：GB/T 25070-2019[S].北京：中国质检出版社，2019.

[9] 国家市场监督管理总局，中国国家标准化管理委员会.信息安全技术 网络安全等级保护测评要求：GB/T 28448-2019[S].北京：中国标准出版社，2019.

[10] 国家市场监督管理总，国家标准化管理委员会.信息安全技术 信息系统密码应用基本要求：GB/T 39786-2021[S].北京：中国标准出版社，2021.

[11] 霍炜，郭启全，马原.商用密码应用与安全性评估[M].北京：电子工业出版社，2020.

[12] 埃文·吉尔曼，道格·巴斯.零信任网络 在不可信网络中构建安全系统[M].奇安信身份安全实验室，译.北京：人民邮电出版社，2019.

[13] 何国锋.零信任架构在5G云网中应用防护的研究[J].电信科学，2020，36(12):123-132.

[14] 冯九龙.政务大数据助力智慧城市精细化治理[J].大科技，2021(16):274-275.

[15] 张明斗，刘奕.基于大数据治理的城市治理现代化体系研究[J].电子政务，2020(3):91-99.

作者简介：
刘毅，硕士，主要从事移动政企安全管理工作；于乐，博士，主要从事网络信息安全风险管理工作；张峰，教授级高级工程师，博士，主要从事网络信息安全管理工作；马禹昇，硕士，主要从事网络安全、工业互联网安全等工作；林艳纯，工程师，硕士，主要从事ICT业务相关咨询工作。