热点追踪

6月26日，在江苏南京网络通信与安全紫金山实验室，全球首个网络内生安全试验场正式向首批100名国内外申请者开放通道，接受网络安全技术爱好者的国际性大众测试。该试验场基于我国科学家原创的网络空间拟态防御理论和技术研发而成，是推进从源头解决网络安全问题的先进技术代表。此举开创了一种网络安全产品的全新认证模式，有助于消除全球化供应链、产业链中的网络安全壁垒，推动网络空间命运共同体建设迈向更高台阶。

首个面向全球开放的网络安全防御技术试验场正式运行——

为网络空间安全提供“中国方案”

■本报记者 张 锋

真金不怕烈火炼——

开放平台彰显技术自信

NEST这样一个英文缩写，很容易让人联想到2008年北京奥运会主场馆“鸟巢”。现场专家开玩笑说，当年北京奥运会因为“鸟巢”国家体育场倍添光彩，被誉为“无与伦比”的一次奥运会。如今，网络空间的“鸟巢”开展国际众测，是否也会产生“无与伦比”的效果？

原来，网络内生安全试验场（NEST）是基于我国科学家原创理论和技术研发的。所谓网络内生安全，是指依靠网络自身构造因素产生的“测不准”效应，获得传统与非传统安全功效，犹如人体自身就具有对多种病毒、细菌的非特异性免疫功能。

其技术根源，是网络空间拟态防御具有上述内生安全属性，与现有网络安全和防护技术的“亡羊补牢”防御思路截然不同的是，它将安全、可信的“基因”赋予在网络信息系统和设备诞生之初。

据该理论的提出者、中国工程院院士邬江兴介绍，该理论通过内生的“测不准”效应，可以使按此设计的软硬件系统在不依赖“附加”或“外在”防御措施的情况下，就能有效抑制隐藏在系统内部的漏洞后门、病毒木马等安全威胁，可在全球化供应链“有毒带菌”的条件下，提供稳定可靠、安全可信的系统服务。

近年来，网络空间拟态防御技术迈出的每一步都踏实有力，从理论提出、原理验证、技术突破、设备研制均取得了全方位进展。2016年，拟态防御原理验证系统通过国家级测试评估；2018年，全球首例基于拟态构造的系列化网络设备投入线上运行。

去年以来，在南京举办的两届“强网”拟态防御国际精英挑战赛上，拟态系列设备共计封堵了顶尖“白帽黑客”的340余万次攻击，无一漏网，在真实网络场景下初步验证了其安全属性。

如今，紫金山下再次摆开“英雄擂”，欢迎全球高手随时来战！这样的底气、勇气和霸气，预示着又一轮鏖战即将上演。

狭路相逢勇者胜——

开创人机对抗新模式

大战在即，NEST已经做好了准备。那么，处于攻击侧的“勇士”从何而来？记者在现场研究了该试验场的运行规则和机制，亲身体验到主办方细致的准备。

从事网络安全的个人、组织都有着鲜明的个性，我们暂且可将其定义为“黑客文化”。在这个文化体系中，“技术、挑战、自由”是他们普遍追求的理念。

所以，该试验场将测试对象确定为我国独创的网络空间拟态防御技术，其具体目标环境，涵盖了拟态路由器、拟态域名服务器、拟态文件存储系统、拟态Web服务器、拟态防火墙等多款设备。主办方在报名主页上还提供了该技术的原理介绍，以及应用场景示意图等信息，为挑战者提供了便捷贴心的服务。

如此开放的测试平台，可谓“火药味”十足。网络安全从业人员、红客、“白帽黑客”为了维护正义，必然参赛；网络世界鲜为人知的黑客们，收到这份“战书”也同样会跃跃欲试。

曾经，高尔丁死结被亚历山大大帝用创新规则解开；两千多年后，又一个“改变游戏规则”的技术及其运作模式诞生。

犹如海纳百川，全球网络空间传统正义力量和“非正义”力量将在此处“交锋”，为安全技术验证和能力提升贡献智慧。

办法总比困难多——

重建网络安全信任机制

中国有句老话：三十年河东，三十年河西。

信息技术发展和全球化进程相促相生，都曾被人们视为充满无限生机、无尽财富的“阿里巴巴的山洞”。

但与此逆向而行的是，网络产品的安全问题现状基本是“自说自话”，缺乏权威的国际性第三方机构，所以A可以对除了自己以外的B、C等任何一个组织设计、生产、制造的设备产生不信任，树起了信息化、全球化过程中一道道无形的障碍。

因此，网络安全问题近年来被一些人看作“潘多拉的盒子”，与之伴生的逆全球化行为，与世界和平、发展、合作、共赢的时代潮流背道而驰。这绝不是大家想看到的。

但又如我国的另外一句古话所说，“不可因噎而废食。”网络安全问题必须予以高度重视，采取“釜底抽薪”的有力举措，消除扩大化的保护主义、单边主义的不利影响。

NEST在这方面的作用将是基础性、核心性的。据邬江兴院士介绍，该试验场将成为可靠、可用、可信信息技术产品的“试金石”，为消除国际间因网络安全问题形成的壁垒和鸿沟发挥重要作用，为实现网络空间互联互通、共享共治，推动网络空间命运共同体建设迈向更高水平——

从此，网络设备产品的安全测评，不再是谁设计谁验证，而是有了一个全球性、开放式的众测平台；

从此，网络内生新一代信息安全技术正式向全世界展示其功能效果，将带动全球信息技术与产业实现升级换代；

从此，网络安全人才培养、产业促进、技术进步将在一个试验场内实现。

邬江兴院士说，我们始终坚信，办法总比困难多。世界必将因连接万物的互联网而多彩，人类生活必将因安全可信的互联网而更加丰富。

上图：网络安全学科竞赛现场。

图片由紫金山实验室提供

什么是网络内生安全试验场

“网络内生安全试验场”（NEST），是由网络通信与安全紫金山实验室创建，国际上首个永久在线、面向全球开放的网络安全防御技术试验场。该试验场将为各类网络设备和信息系统提供全球性众测平台，对被测设备的安全指标进行全面度量，为“红蓝式”网络攻防对抗演练提供近似真实环境的试验性网络，也可为网络安全从业人员提供全面技能培训。

NEST聘请第三方机构负责在线运营，随时欢迎来自全球的个人和组织挑战。同时，试验场将向全球提供技术验证、安全比赛、能力评价等多项服务，打造全球网络安全新高地，孵化多样化的技术产品，用创新技术和实践效果推动网络空间安全建设不断取得新进展。

NEST首批提供了4款产品众测场景和1项体系化应用众测场景，依据报名用户的信息来分配测试时段和测试场景，采用有偿众测模式，第一年度奖金总额为150万元人民币。

NEST系统测试的目标环境，包括众测单个设备场景和众测设备体系化应用场景。单个设备场景包括：路由器场景、域名服务器场景、文件存储系统场景、Web服务器场景。众测设备体系化应用场景由防火墙、路由器、域名服务器、文件存储系统、Web服务器构成。防火墙连接路由器，路由器下联域名服务器、文件存储系统和Web服务器。

加快推进网络安全学科竞赛创新发展

■中国工程院院士 邬江兴

1996年，全球黑客大会首次推出CTF竞赛模式。这种在特定平台上进行攻防竞技的方式，代替了之前黑客通过互相发起真实攻击进行技术比拼的方式。

自此，在学科竞赛的辞典中出现了“网络安全学科竞赛”这个名词。经过30多年的发展，CTF已经风靡全球并在中国得到蓬勃发展。据统计，2018年我国的CTF竞赛已经超过1000场。

然而，网络安全学科竞赛繁华之后如何发展？如何与网络强国战略有机结合？值得人们深思。

今年5月22日至23日，紫金山实验室举办了拟态防御国际精英挑战赛，29支国际顶级战队在20小时内，向6款拟态设备发起290万次大强度攻击。这次比赛最大的亮点，是建立了一种“人-机对抗”的网络安全竞赛模式，颠覆了传统“人-人对抗”的CTF竞赛模式，网友们比喻这是国际黑客大战“摩托狗”。

这一对抗模式，我们称之为“BWM”模式，是现有网络安全竞赛的第四种模式，不是游戏，不是“挖洞”，也不是水平认证，而是基于开放性众测的一种竞赛模式。

竞赛的主体不是人与人，而是人与机器。传统的CTF以及其他竞赛模式，对抗的主体是人与人。BWM赛制，对抗的主体是人与机器，是通过设置一个合理的竞赛场景和竞赛规则，检验人的网络攻击能力是否能够突破具有内生安全功能的网络设备，这就如同围棋界的人机大战一样。

竞赛的载体不再是题目，而是网络设备。BWM赛制一经亮相，参赛选手第一反应就是：没有赛题了。事实上，这次上线的6款拟态构造COST级设备就是赛题，这里面蕴含着“一生二、二生三、三生万物”的哲学思辨能力，有着无穷无尽的赛题，选手们依靠自己的思维“发现”题点，依靠自己的判断“攻克”题点，没有题目的比赛，更加富有探索性和挑战性。

竞赛的目的不仅仅是选拔和锻炼人才，而是赋予了科学度量网络产品安全性的新职能。传统基于人的网络安全竞赛，其核心是发现和锻炼人才，有的网络安全竞赛往往被“猎头”公司所青睐。

竞赛的确可以发现人才，但是这些天赋异禀的人仅仅用来打比赛显然是不够的。在BWM模式中，巧妙地引入了众测的理念，大大提升了比赛的效益，使得用竞赛来度量网络产品的安全性成为了可能。

竞赛的方式也不再是一锤子买卖，而是常态化测试和集中式竞赛的有机结合。这次拟态精英挑战赛同时发布了永久在线的内生安全试验场，从6月26日开始，全天候接受全球“白帽黑客”的有奖众测。未来的比赛，可能是常态化、无差别的竞赛，鼓励更多有创意、有兴趣的技术专家去挑战各种“不可能”。

竞赛的焦点不再是漏洞，而是推进共享共用共建。在BWM模式下，零漏洞后门已不再是制胜法宝，你甚至可以自己预先布设一个漏洞后门乃至病毒木马，因为拟态构造系统对已知或未知的病毒木马具有天然免疫力。这种模式不以拥有的漏洞资源多寡为前提，不必担心信息资源泄露，也不用顾忌境外顶级黑客的参与。共同的挑战是：如何在拟态构造的“测不准”环境内，形成非配合条件下动态多元目标协同一致的稳定逃逸机制。倘若人类无法战胜“摩托狗”，则打造网络空间命运体就有了可靠的技术抓手。

未来的网络安全学科竞赛，将会实现多种模式共同发展，CTF类的比赛也会不断改革，BWM模式将作为非CTF模式的比赛走向前台。未来的竞赛不再是游戏，而是服务产业和技术发展，为建设网络强国服务。

论见

发挥国家战略科技力量建制化优势

■陈 套

建制化的国家战略科技力量，是大科学时代科学研究的显著特征，更是科技创新范式转变的必然选择。国家建制化战略科技力量在提升基础科学研究能力、解决国家战略安全、战略需求问题和推进高质量发展方面具有不可替代的作用。

建制化加速了科技发展。科学技术研究作为社会建制诞生于19世纪，发展于20世纪。大体上，18世纪主要以个体研究为主，19世纪逐渐形成集体研究体制。进入20世纪40年代以来，国家规模研究和国际合作研究成为主流。

从国际历史经验来看，世界科技强国都拥有自己的国家战略科技力量，用来部署前瞻领域研究，抢占科技战略制高点。德国的普朗克科学促进学会、亥姆霍兹联合会、弗朗恩霍夫促进会、莱布尼茨联合会汇聚了众多一流科学家。法国组建了国家科研中心、国家农业科学研究院、原子能委员会等。

发挥国家战略科技力量建制化优势，必须从战略导向、政策引领、平台建设、基础研究、科学精神等方面着力加强。

坚持战略导向、问题导向和目标导向。大科学时代原始创新重大成果的取得，有赖于国家战略科技力量建制化优势的充分发挥。发挥国家战略科技力量在组织重大科技攻关中的龙头作用，应聚焦国家科技创新战略需求，保持科技战略定力，发挥科技预见作用，强化在战略性研究、国家重大科技任务、科技咨询和服务等方面的创新政策引领。

建设科技创新重大集聚平台。应集中国家科研力量建设好国家实验室、重大科技基础设施集群和综合科学中心，明确国家战略科技力量建制化的创新布局和功能定位，强化国家战略科技力量肩负国家创新发展的历史使命和责任担当意识。重大科学工程和平台对人才具有磁场效应，应发挥好先进科研平台汇聚人才的作用，为优秀人才创造良好的科研条件，形成人才相互影响、相互促进的“共生效应”。

提升基础性科学研究能力。应重视和支持原始性创新和关键技术的自主创新与系统集成，优化经费投入结构，摆脱平均主义科研思想的束缚，重点加强基础性科学研究。坚持重大成果和引领创新的评价导向，积极参与组织国际大科学工程和计划，力争成为全球科技创新的领跑者。

成为科学精神、科学文化和学术生态的引领者。应通过发挥国家战略科技力量建制化优势，强化使命驱动和价值驱动，将创新精神内化为人的一种意志力量，激励科研人员主动作为、敢于担当，成为科学共同体自律的引领者，实现科技与道德互相促进、良性互动。