

# 拟态防御：让黑客找不到破门之机

文·本报记者 何亮

继10月美国网站大规模宕机后，当地时间11月27日欧洲最大电信运营商德国电信又遭受严重攻击，导致约90万路由发生故障，连续两日断网。

物联网时代，当所有的设备都变成智能化，都接入网络后，边界的概念将会进一步被削弱。而万物互联，使得网络安全形势非但没有减弱，相反愈发严峻。

木，通过拼装组合成不同的“计算装置”（比如计算机、计算尺等）。系统通过策略调度和多维重构，动态地生成富于变幻的“计算装置”组合。当执行指令时，“计算装置”的组合处于复杂变换状态，而装置的功能从未改变。巧妙的是，从系统外观察，计算装置的漏洞与后门随着装置的变换而不停地变化。漏洞成为瞄不准、测不到、打不着的存在，漏洞的缺陷也就无法被有效利用。

让“计算装置”的漏洞失效是有前提条件的，即计算机、计算尺、算盘等执行体是网络设备的软、硬件，自身都存在漏洞缺陷并具有相同的功能。漏洞失效的机理在于，当三个装置同时执行2×3的指令后，系统只输出多数相同的结果。如果三个结果均为6，输出结果为6；如果一个为5、两个为6，这时5为少数，输出结果仍然为6。“其实，这样的算法并不知道什么是对、什么是错，只是按照多数还是少数执行。其巧妙之处在于，不知道各个装置有什么问题，只知道很难出现同样的问题。” 鄂江兴说。

相比传统精准防御，拟态防御不以弄清木马病毒与漏洞后门的性质为前提，不依赖于先验知识——不断更新的病毒库，而依靠系统的内生防御技术。同时，随着执行体的快速变化，设置在执行体中的后门成为了一个“转门”，攻击者连入口都无法找到。总之，系统通过快速选择不同功能的组合执行体，在变化中完成给定的任务，使单位时间内攻击者做出的攻击决策既不能一招制敌，又在短时间内迅速失效。这时，不确定性威胁就变成一个极小概率的网络攻击事件。

## 拟态防御并非“神乎其神”

调拟态防御的适用范围。

鄂江兴进一步解释，实现拟态防御的前置条件包括四个方面。首先其冲是要存在可判定异构冗余体之间功能等价性的“拟态界”，还需要在给定功能性能下存在软硬件多元或多样化供应条件；再就是该技术适合于兼具高安全性和高可靠性的应用领域，比如交通、电力、能源、国防这些领域。

此外，由于拟态防御系统要求同一功能的多构件组合，相比单一构件系统，成本大幅增加。因此，在初始阶段，拟态防御的投资回报率不高，更适用于高成本投入的安全领域。

## 四处“漏风”的安全防卫系统

根据国家互联网应急中心抽样检测数据显示，仅2015年我国就有1978万多台主机被10.5万多个木马和僵尸网络控制端控制，2015年检测到的浏览器漏洞数比2014年高出37%，操作系统漏洞数高出73%。事实说明，我国已成为遭受网络攻击最为严重的国家之一。

虽然防护措施不断更新迭代，却依旧无法对抗黑客，症结在何处？

计算机与网络技术专家、中国工程院院士鄂江兴在接受科技日报记者采访时表示：“网络安全问题复杂而多变，这些问题当中造成网络安全防御‘易攻难守’的主要技术原因是，

现有的科技水平尚未形成穷尽与彻查信息系统软硬件代码问题的理论与方法。而且，现有防御体系的脆弱性加上免疫机制的缺陷，再加上信息系统的基因问题，共同构成网络空间最大的安全黑洞。”

面对这些隐身于各处的未知漏洞、后门，首先是无法用概率表示，其次是现有计算机根本对它探测不准。即便采用入侵检测技术、防火墙技术、密码加持技术构筑起一道道“铜墙铁壁”，如果感知不到具体威胁在何处，就等于形同虚设。比如，漏洞或后门设置在机密机的底下，加密技术被轻易绕过，密码成了摆设！

## “七十二变”让攻击者失去目标

在太平洋，有一种“聪明”的生物叫条纹章鱼。据说，它能模拟至少15种海洋生物，通过变换颜色、条纹等迷惑攻击者，降低攻击的有效性，就像孙悟空的七十二变。

鄂江兴将这种防御策略称为“拟态防御”，并借用钱学森的系统工程思想——“从复杂问题的总体入手，认为总体大于各部分之和，各部

分虽较弱但总体可以优化。”也就是说，忽略各个构件存在的漏洞，从总体上将生物界的拟态防御原理导入网络安全领域，构建一种新的网络防御系统，即功能等价条件下异构冗余多动态重构机制。

这一复杂的信息防御体系，其特别之处在于系统中放一个构件池。构件像小孩玩的积

2016年8月，由53位同行专家（包括13名院士）署名的《拟态防御原理验证系统测评意见》正式公布，测评结果表明：现有的扫描探测、漏洞利用、后门设置、病毒注入、木马植入乃至高级持续威胁（APT）等常规或非正规攻击手段方法，对拟态界内受保护对象没有预期的作用和可信效力。有媒体给出高度评价：“拟态防御或将是网络安全与信息化融合领域的‘游戏规则改变者’！”

“任何事物都不可能‘神乎其神’，‘拟态防御’拥有明显的创新性，但不是放之四海皆准的原理。”作为理论的提出者，鄂江兴特别强

## ■聚焦

# 潜心钻研 厚德勤奋

## ——记中国电建华东勘测设计研究院院长张春生

文·陈雷 杨蕾芳

作为中国电建华东勘测设计研究院院长、中国电力行业优秀企业家，张春生从事工程设计与技术管理工作30年，主持和参加了二十余项国家重点水电水利工程的勘察设计工作，为我国水电水利工程设计、咨询、技术标准与关键技术难题攻关等领域做出了重要贡献，先后获得国家级科技进步奖、国家级优秀设计金奖等众多奖项。

他个人被授予国务院政府津贴专家、全国五一劳动奖章、全国电力勘测设计行业资深专家、浙江省工程勘察设计大师、浙江省有突出贡献中青年专家……

这些荣誉如大地纹理般清晰而厚重地记录下张春生投身水电事业30年来所取得的成就。

作为企业的掌舵者，张春生高瞻远瞩、洞悉形势、矢志事业，以技术服务为立业之基，科技进步为强院之本，始终将国家和为业主服务的使命铭刻心中，在服务工程、服务企业、服务员工、服务社会的道路上披荆斩棘、执着前行。

日前，张春生荣获“中国电力科学技术杰出贡献奖”。

### 攻坚克难 勇攀世界水电技术高峰

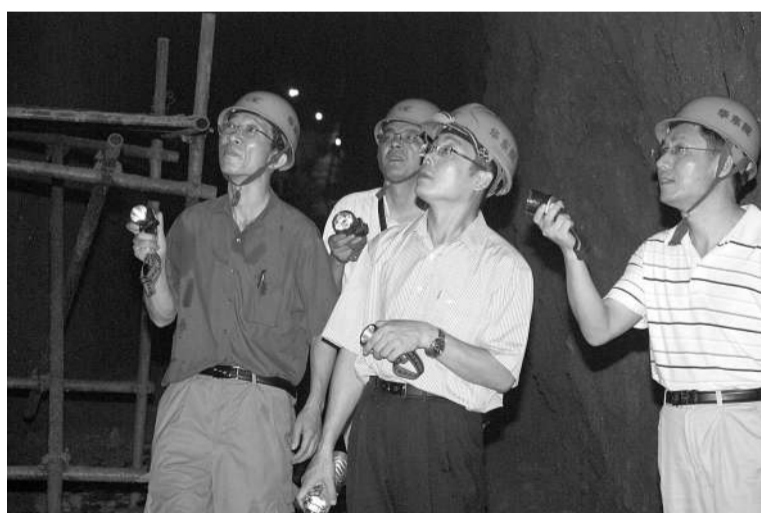
多年来，华东院致力于大型水电工程的科研攻关，攻克了一项项世界级水电技术难题。张春生作为多个国家大中型重点项目负责人，致力于科技创新，极大地提升了华东院在大型水电项目领域的科研技术水平。

锦屏二级水电站是雅砻江上装机规模最大的巨型水电站，拥有世界上综合规模最大的、技术难度最高的水工隧洞群。华东院为之结下了近半个世纪的情缘。

2003年，张春生担任锦屏二级水电站设计项目经理，全面主持锦屏二级水电站关键技术研究工作。水电界有句话：摇头容易点头难。对于一项复杂的问题，提出意见和质疑很容易，但要解决问题做出决策就难了，意味着要准备承担各种责任和后果。

2009年，现场发生突涌水，水流湍急，洞内积水一直到胸口，水温只有几度，冰冷彻骨。为在第一时间查明险情，张春生带领技术人员在水中一站就是几个小时，把现场情况掌握清楚后才肯罢休；晚上则连夜组织技术攻关，经过不懈的技术攻关，成功实现了地下水封堵，保证了工程的施工安全。

他凭借着扎实的理论基础、丰富的实践经验和敢于担当的气魄，带领华东院人相继克服了高地应力和强烈岩爆等一系列世界级的技术难题，创造了多项世界纪录，为锦屏电站的顺利建设奠定了坚实的理论和实践基础，并推动我国深埋长隧洞建设技术迈上了一个新的台



张春生（右二）在白鹤滩工程地下洞室。

阶，研究形成的《深埋高外水压力水工隧洞关键技术研究及应用》等系列技术成果，达到国际领先水平。

锦屏工程完工后，2012年，张春生作为设计项目经理又投身到千万千瓦级巨型水电站——金沙江白鹤滩水电站的建设和技术攻关中，开展的国际上首台单机容量百万千瓦级机组的研究，全面提升了我国水力发电设备企业整体生产能力和技术水平。

抽水蓄能业务是华东院响当当的一块牌子。上世纪九十年代，张春生作为项目设计总工程师全面参与了浙江省安吉天荒坪抽水蓄能电站的设计和重大技术问题决策。天荒坪水电站是目前我国已建单个厂房装机容量最大、设计水头最高的抽水蓄能电站，工程首创了多项工程设计和施工技术，为我国蓄能电站排水设计出了一条新路。

之后，他又主持完成了山东泰安、江苏宜兴等抽水蓄能电站的设计，先后承担了“面板堆石坝坝身溢洪道技术研究”等复杂条件下抽水蓄能电站建设系列关键技术攻关，突破了库盆防渗等技术难题。整体技术成果达到国际领先水平，技术成果全面推广应用到桐柏、泰安等十余座国内大型抽水蓄能电站建设。

近年来，张春生还将在国内水电工程中积累的技术和经验不断拓展到了国际水电市场。目前华东院已经累计承接近百个国际工程项目，区域遍及越南、土耳其、新加坡、泰国、尼日利亚等四十多个国家，业务涉及水电站、输变电、水利项目等设计咨询、机电成套

以及工程总承包等多个领域。

### 求真务实 服务区域重大发展战略

作为一家地处浙江的中央企业负责人，张春生带领华东院主动对接浙江省重大发展战略，积极响应浙江省“四大国家战略举措”“四大建设”要求，在推进国家和浙江省重点工程建设和重大科研项目方面作出了突出贡献。

近年来，受浙江省能源局委托，华东院相继承担了浙江省抽水蓄能规划、省潮汐能规划、省海上风电工程规划、省（舟山）海洋能（潮流能）规划等，为政府和有关单位建设了7座海上测风塔，完成了浙江省内6个海上风电项目可行性研究报告。

2010年，为更好地响应浙江省海洋战略，服务于舟山群岛新区为核心的海洋经济发展需要，华东院先后参与浙江省小岛屿开发研究、浙江省海岛能源保障课题研究、海岛孤网和并网型能源利用研究、海岛核能开发前期研究、海洋环境保护研究等多个科研项目。也是在这一年，华东院被列入国家第一批海岛保护规划编制技术单位推荐名录。

2011年，华东院在浙江舟山成立了舟山分院，派驻了一批高层次、高学历的管理人员和专业技术人员，直接服务于浙江省海洋发展战略，先后完成了国内首个综合利用风能、太阳能、海水淡化的舟山福山岛工程，华东地区最大的舟山六横岛10万吨海水淡化工



张春生（左二）在项目工地。

程，以及海堤、船坞、渔港等数十项涉海工程的勘察设计咨询工作，推动浙江海洋经济和舟山群岛新区亮相中国海洋经济大舞台，为我国和浙江省的海洋经济建设做出了显著贡献。

近年来，张春生还带领华东院积极参与市政建设，先后承担了杭州市杨公堤恢复工程、天目山路、延安路等综合整治工程，杭州地铁、紫之隧道、环西湖隧道群、印象西湖、金沙湖下沉广场、钱江创新产业园、南宋官窑遗址工程，以及道路、桥梁、码头等百余项工程的勘测设计和总承包业务。此外，还承担了浙江宁波、象山、玉环、三门、开化、丽水、江山、常山、桐庐、诸暨、缙云等地区的一大批污水和固废处理工程，有效缓解了杭州交通拥堵现状，改善了省市生态环境，为积极推进五水共治、绿色发展、循环发展、建设生态浙江和美丽浙江做出了积极贡献。

### 科技引擎 打造科技创新一流企业

科技创新是一个艰苦复杂的过程，要耐得住寂寞，抑制浮躁。无论是作为总工程师还是院长，十余年来，无论遇到多大的质疑和阻碍，张春生始终坚守着科技和创新和技术进步的底线不动摇。他坚信“只要是正确的道路，就要一条道走到黑，这样才能真正落在实处”。在执着追求下，2003年，科技战略作为院发展战略体系的第四项子战略首次正式提出，并将实施科技战略与经营战略相结合，坚持以技术竞争力来促进经

## ■IT辣评

点评人：本报记者 王小龙

## “香艳”的圈子 不过是巨头之间的新战场



11月25日，支付宝的“圈子”功能尚处于测试阶段就引来了大量关注。仅仅“校园日记”和“白领日记”这两个圈子，就聚集了2000万关注者。随着数字不断上涨，圈子里开始出现了大量大尺度照片。由于这两个圈子在功能设置上的导向性非常明显，支付宝也被指有借势炒作之嫌。

点评：以前，微信是微信，支付宝是支付宝；后来，微信越来越像支付宝，支付宝越来越像微信。原先它们各有所长，如今都谋求“加特技”，试图进入对方支配地位的领域。就像微信不甘心只做社交，支付宝也不愿只做一个“安静”的支付工具。

2014年，借助强大的“社交基因”，微信红包一经推出就火遍全国，绑定微信支付的用户激增，打破了支付宝一家独大的局面。自己的地盘被占，阿里巴巴痛定思痛，将原因归结于两个字——“社交”。微信红包给支付宝上了一课，让支付宝对用户黏性的认识提升到一个新高度。支付宝高层曾多次表示，支付宝并不是不知道用户只想要一个简单而好用的支付工具，但“人在江湖身不由己”，只做支付，是方便了用户，但“支付宝可能就要死了”。

事实也确实如此，目前微信的月活跃用户已超8亿，而支付宝用户不过4.5亿。根据易观的数据，自2015年至2016年第二季度，支付宝市场份额由68.4%降至55.4%，而与此同时微信支付的服务方财付通则由20.6%升至32.1%。

微信步步紧逼，支付宝诚惶诚恐。要想生存，只有主动进攻。在社交领域经历多次失败后，支付宝才发现自己还有几张“好牌”没出，那就是用户大数据和以芝麻信用为基础的信用体系。这两个工具不但能给出清晰的用户画像，还能把那些有相同爱好、共同需求的人聚在一起，建立起以信用为基础的“陌生人社交”。支付宝9月底正式上线的“到位”和这次惹祸的“圈子”都是基于这一思路，对这一战略的布局。

两个“圈子”的规则设置得极为巧妙，只能由女性用户发表内容。男性用户不能发布日志，但可以阅读、点赞、打赏，芝麻信用达到750分以上才能评论。可以说在设计初衷上，它就是冲着“爆款”去的，火了也很正常。

如今，圈里的美女已经“下架”，“吃瓜群众”也已散去。支付宝母公司蚂蚁金服董事长彭蕾发信作出道歉，表示会“深刻反思”。

辣评君相信，在这之后“圈子”里的美女必会有所收敛，但支付宝在社交上的进攻绝对不会就此止步。

（图片来源于网络）