高技术前沿

当我们专注于软件层面的病毒或恶意代码时，可曾想过大量隐藏在芯片中的“硬件木马”来袭？新年伊始，信息安全领域就被一个“重磅炸弹”引爆。1月初，全球著名芯片供应商英特尔公司被爆出处理器存在底层设计缺陷。此次爆发的芯片安全漏洞，被业界命名为“幽灵”和“熔断”，这些漏洞允许恶意程序窃取存储于其他正在运行的程序内存中的数据。由于牵扯到英特尔、ARM、AMD等几乎所有的芯片供应商和各类操作系统，或将成为继“千年虫”之后信息安全领域危害最大的安全漏洞。这进一步警醒我们：掌握芯片这一核心技术的“话语权”刻不容缓！否则，说不定什么时候，有人就会按下潜伏在计算机芯片中的“死亡按钮”。

小心！你的电脑有“芯”脏病

■张乃迁 许玥凡

“瞒天过海”
有意无意设计的“乌龙”

揭开此次英特尔芯片“漏洞门”大幕的，是谷歌公司旗下的“零项目”团队，他们将发现的内核级漏洞分别命名为“幽灵”与“熔断”。这两个漏洞主要涉及到处理器芯片的内核管理机制，就好比我们把贵重物品锁在保险柜中，但依旧有人能找到保险柜钥匙并从中窃取物品。

“幽灵”与“熔断”为黑客提供了保险柜存放位置的“蛛丝马迹”。一旦攻击者利用相关漏洞对处理器展开攻击，就可“越界”访问系统内存，从内存中查看到相关信息，导致用户的敏感信息遭到泄露。更令人不安的是，英特尔公司此次爆发的芯片漏洞，牵扯到自1995年以来所有的X86构架处理器，甚至连AMD、ARM等在内的众多厂商芯片都未能幸免。

其实，这已经不是英特尔公司的第一起芯片“丑闻”了。早在1994年就开始接连出现诸多漏洞与设计“乌龙”，此后的“安腾”处理器也存在着因设计缺陷而带来的时钟频率发生故障。就在2017年上半年，英特尔公司处理器中的主动管理技术、标准可管理性和小型企业技术相关固件都暴露出易遭受远程攻击的漏洞。然而，这些漏洞早在2010年就存在于英特尔公司的部分芯片当中，或许早就被黑客用于开展远程控制攻击。

英特尔处理器芯片包含有管理引擎技术，主要基于迷你操作系统MINIX3研发，相当于处理器内部的一个小型“独立王国”。这个看似迷你的操作系统拥有一整套底层运行机制，英特尔公司还“热心”地为其预留了检查操作系统、管理员远程控制等诸多功能。这个漏洞一旦被攻击者利用，便可用来加载、执行任意代码，且整个攻击过程操作系统都是在用户毫不知情的情况下进行的，真可谓“瞒天过海”。

“预留后门”
软的不行就来“硬”的

从手机、U盘、计算机等普通产品，到飞机、导弹、卫星等军用装备，随着信息技术的快速发展，集成电路和处理器芯片正日益成为现代社会和国防军事领域的关键“核芯”。此次爆发的“漏洞门”事件，也折射出信息安全领域的巨大黑洞。

早在2008年，英特尔公司就已经开始使用管理引擎技术。对于这个拥有极高权限的漏洞及其潜伏已久的安全隐患，英特尔公司不可能毫不知情。若不是此次漏洞事件被媒体曝光，存在巨大隐患的“漏洞门”极有可能被再次“大事化小”。硅谷的信息安全专家指出，生产商在发往某些地区的处理器芯片中或许故意留下后门，以便可以轻易监视计算机用户的一举一动。事实上，在海湾战争期间，美国特工就通过固化病毒程序芯片对网络打印机上演了“狸猫换太子”的好戏，致使战争爆发后伊拉克防空指挥系统全面瘫痪。

近年来，随着人们对计算机系统和软件安全防范意识的提高，在硬件设备中预留后门或植入病毒，成为开展网络攻击的有效办法。早在1998年就曾出现过专门破坏电脑硬件的CIH病毒，近年来寄生在二手主板上的“谍影”病毒也“现身江湖”，同样可实现黑客的远程控制。在2007年“果园行动”中，以色列空军悄无声息地突破叙利亚防空系统，对叙境内纵深地带实施精确轰炸，而确保以军安全返回的“功臣”，竟是芯片制造商提前在叙利亚的军用雷达处理器中加入的远程控制“开关”，致使叙防空雷达在以军到来时临时关闭。

目前，在芯片中植入“硬件木马”开展网络攻击，早已成为公开的秘密。一旦“硬件木马”被远程“唤醒”，就将造成芯片报废，干扰系统正常运行，或“悄无声息”地开展数据窃密，将使信息网络系统无密可保。信息领域的安全黑洞，也将因此成为“无底洞”。

“刮骨疗毒”
自主可控是“治本”之举

尽管目前英特尔、微软、苹果等处理器芯片、操作系统和终端厂商都针对“漏洞门”纷纷给出“打补丁”指南，但依旧不是“釜底抽薪”的长久之计，黑客只需很简单的手段就可攻击用户的存储系统。更何况，英特尔公司针对“管理引擎”漏洞给出的解决方案，竟然也是把管理引擎技术限制在只读模式中，想关闭处理器中的“操作系统”愈发不可能。可见，一个在信息领域长期无“芯”的国家，只能默默吞下芯片“后门”带来的苦果。

如今，“网络军火”的泛滥已成为悬在信息领域上空的“达摩克利斯之剑”。2017年爆发的勒索病毒，在短短24小时内就导致全球150多个国家的数10万台电脑遭受厄运，涉及金融、医疗、电信、能源、交通、政府等诸多部门。美国早就提出“网络数字大炮”概念，据报道目前已研制出可长期潜伏的数千种病毒武器，都是威力巨大的“定时炸弹”。据悉，在国防部高级研究计划局“半导体先进技术研发网络”项目资助下，美国研究人员正开展处理器后门植入技术研究，以进一步获取可攻击芯片系统的能力，或将打造出新一代“硬件木马”。

面对信息安全领域的巨大风险挑战，即便是技术实力雄厚的国家也难逃被“黑”的命运。对此，俄罗斯开展了“厄尔布鲁士”“贝加尔湖-T1”等国产芯片研究，其自主可控的操作系统也于2018年开始列装俄军自动化军事指挥系统和办公电脑。这启示我们：必须加快信息基础设施领域自主可控产品的研发与应用，对电脑“芯”病进行“刮骨疗毒”！

制图：郭烨瑾

论见

在颠覆性创新中走向『神速』

■贾玉树 杨玉瑞

中国自古有“兵贵神速”的说法。然而何谓神速，并没有一个明确的阐释。一般说来，它应当在极短的时间内通过极长的距离，其结果超出当时人们所能想象的范围。由于速度涉及时间和空间两个方面，所以，它取决于特定时代科学理论在时空领域中技术开发的水平。

纵观人类战争史，速度始终是军队克敌制胜的不二法门，包括移动速度、打击速度、保障速度与通讯速度等。从某种意义上讲，国防科技史也始终是以速度为核心展开的。因为它在不断扩展人类活动空间的同时，也在缩短相应的时间。

冷兵器时代，短兵相接，谁能够以迅雷不及掩耳之势袭击对方，或在更短的时间内把更多的兵力投送到前线，谁就有望夺取胜利。热兵器时代，军队开始在越来越远的距离作战，科学技术第一次在人类历史上释放出巨大的物质力量。如果说，拿破仑时代火炮与骑兵的协同速度还带有浓厚古代色彩的话，那么第一次世界大战出现的坦克、汽车、舰艇、飞机等则揭开了现代战争的序幕，第二次世界大战更是把“闪电战”演绎得淋漓尽致。从此，科学技术变成了第一战斗力，“主宰”了人类战争。

接踵而来的是信息化时代。现代科技突破了第一宇宙速度、第二宇宙速度，战场从天空延伸到太空，形形色色的航天器时刻俯瞰着“地球村”里的一举一动；各种各样的无人系统开始取代人类纵横驰骋在万里疆场，对传统作战方式产生了“颠覆性”影响。与此同时，国防空间从有形的三维空间伸向无形的多维空间与虚拟空间，高度复杂的战争巨系统全面呼唤军事装备向智能化方向发展，陆、海、空、天、电、磁等不同的时空在颠覆性创新中获得前所未有的统一。

当代国防科技发展的一个重要特点是理性化，即自觉运用现代科技的原理、方法和手段，开发新的时空，寻求快速打击的最佳途径和方法。一方面，按照传统思路发展高超音速飞行器。1996至2002年，美国国家航空航天局（NASA）提出三种“突破性的物理学推进技术方案”，分别基于核裂变、核聚变和反物质湮灭原理来发展超高速飞行器。美国“乘波者”X-51型超音速飞行器利用超燃冲压发动机可能实现最高达25倍的音速，让战争进入“读秒”时代。另一方面，根据全新的科学构想创造出新的速度。早在1994年，物理学家阿库别瑞就曾提出一种通过波动方式延展空间的想法，可以使宇宙飞船以10倍的光速实现星际航行。目前这种方法的可行性已经获得证实，尽管还存在很多问题，尤其是扭曲空间所需要的能量，远不是当代技术能够提供的，然而NASA还是把它列入其研究计划中。

新成果速递

新型加密技术为数据安全加把“锁”

近日，日本一家信息通信研究机构开发出一种新型加密技术，该技术的原理是按照一定规律将密码及信用卡号等需要保护的数字转换成其他形式，即便使用目前性能最高的超级计算机——量子计算机，理论上也至少需要10的50次方年才能解开。它的另一特点就是安装方便，现有的各种通信系统只需更换软件，就能直接使用这项技术。研究人员预言，这项技术将在保护网上交易等机密事项上发挥重要作用。

（赵 欣、何孝林）

人工智能打造战车“移动4S店”

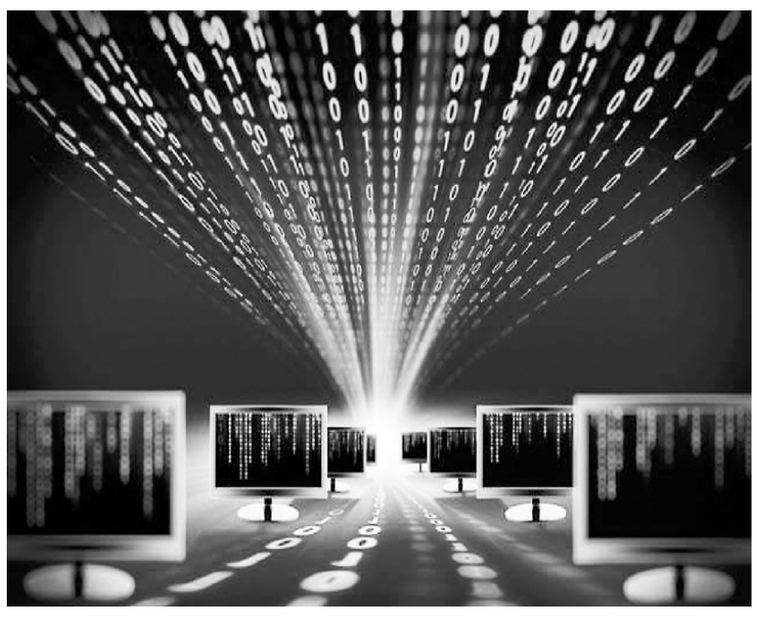
近日，美国《国家利益》网站刊文称，美国陆军武器开发人员完成了一次“原理验证”演习，利用人工智能帮助监控车辆状况，预测车辆未来需求。由人工智能驱动的计算机能够实现对历史数据库和传感器信息的快速读取，使指挥官能够快速掌握机械可能发生的故障、设备运转状况及使用寿命，以便于实时做出决策，相当于为装甲战车打造一个“移动4S店”。

（赵 磊、董浩浩）

依托物联网构建联勤保障“智慧之网”

■王雪诚

兵马未动，粮草先行。这条亘古不变的真理，在信息化战场上同样适用。从近几场战争实践来看，联勤保障早已成为影响部队战斗力生成的重要因素。作为一座尚未探明储量的“富矿”，物联网技术的发展必将触发联勤保障建设的革命性变化。这就要求我们依托物联网技术，构建出一张联勤保障的“智慧之网”。



推动联勤保障一体化

信息化战争的基本作战样式是一体化联合作战，联勤保障符合一体化联合作战的基本要求，是各国军队后勤转型发展的必由之路。物联网可将联勤保障与数字化战场合二为一，实现联勤保障与信息化作战一体化融合，进而实现联勤保障结合作战指挥提前决策、随时部署，可极大程度优化现代后勤保障的流程和组织结构。

同时，物联网还将实现跨军兵种的一体化联勤保障体系。伊拉克战争期间，美军为保证武器装备的高速运转，通过建立地面燃料集结地、雇用油轮和空运航空燃油，实现了油料的高效补给。这得益于美军借助数字信息系统将采集到的油料需求信息和配给信息自动合成、综合处理，已经具备了军事物联网用于联勤保障的雏形。

推动联勤保障可视化

随着军事物联网的快速发展，实现联勤保障态势可视化，打造信息化条件下的“透明战场”将成为可能。借助形式多样的感知设备，军事物联网可融合生成精确、完备、动态、多维的战场联勤态势图，辅助指战员全面准确地了解战场联勤保障情况。通过对战场联勤保障的实时感知和智能控制，有望廓清该领域的“战争迷雾”。

海湾战争结束后，粗放式的联勤保障导致美军在战场上滞留了超过40万吨剩余物资。事后，美军不得不打开清点其中的2.5万个集装箱，直接造成了数十亿美元的经济损失。伊拉克战争期间，美军运往战区的每个集装箱都加装了无线射频芯片，不仅加快了后勤装备补给“从车间向战壕”的运送，更实现了从“储备式后勤”向“快递式后勤”的转变。通过借助物联网技术构建“全球资产可视化系统”，美军在战争中实现了对装备物资的全程跟踪和灵活调配，提升了战场联勤保障水平。

推动联勤保障精细化

随着“非接触”“非线式”等作战样式和“快吃慢”“远制近”“高控低”等博弈思维的快速发展，直达精准的联勤保障已成为物资消耗惊人的信息化战争中争夺胜负天平的关键筹码。

射频识别、二维条码和智能感知技术的实现，推动联勤保障向“动态精确化”方向快速发展。一方面，军事物联网能在地点和时间上精确地向作战部队提供装备补给，避免了多余物资向作战地域的混乱涌入，大大降低了联勤保障工作的盲目性；另一方面，通过嵌入在各类装备和武器平台上的信息传感网络，可实时获取战场后勤需求，根据战场态势修改保障方案，实现对整个保障系统的精准控制。

美军目前正在构建的“感知与反应后勤”系统，就是以物联网为主体，将整个战场空间的态势感知、指挥控制和每一个用户终端连为一体，形成透明、共享、精细、一体的战场联勤保障网络。

推动联勤保障智能化

物联网技术在联勤保障领域的应用，可将大量的人力资源从繁杂的事务性工作中解放出来。据统计，将物联网技术应用于装备存储仓库的智能化管理，原来需要十几人“忙活”一整天的工作，将来只要1到2人花上几个小时就可轻松完成。由于物联网技术实现了人与物、物与物的“智能对话”，因此在实现联勤保障精确高效的同时，也促进了相关军事装备的智能化发展。

目前，西方军事强国已逐步将物联网和传感器网络融入指挥控制系统中，愈发强调战场态势的实时感知与信息的快速处理。随着物联网与人工智能、增材制造、纳米材料等技术的“化学反应”，全自主化智能联勤保障装备或将成为战场后勤补给的主角。未来智能联勤保障装备可向最近的维修中心自主发出零部件需求，各类联勤保障装备甚至还可混搭成后勤保障网，实现战场联勤保障的高效互联互通。

当然，联勤保障物联网建设是一项庞大的系统工程，在建设过程中要充分依靠军民融合，借助民用物联网的力量助推军事物联网快速发展。这就要求我们抓紧研发军事物联网的加密解密、统一身份识别认证和动态授权管理等关键技术，同时采取有针对性的安全保护措施。唯有如此，才能依托物联网构建起战场联勤保障的“智慧之网”。