中国工程院院士邬贺铨：

合作共建网络安全大生态

本报记者 李佳师

> 互联网的安全问题是国际化的问题，需要加强国际合作，维护全球共同的互联网安全生态。网络安全已经是国家、社会、企业乃至个人绕不开的重要命题，需要各个领域以及每个个体携手共建互联网安全大生态，发展网络安全行业是当务之急。

中国工程院院士邬贺铨在第七届互联网安全大会上表示，互联网的发展日新月异，互联网覆盖范围进一步扩大，随着5G时代、万物互联时代到来，新形势下的安全问题也日益严峻，网络攻击造成的影响比过去更为严重。而互联网的安全问题是国际化的问题，需要加强国际合作，维护全球共同的互联网安全生态。

邬贺铨表示，至今，中国互联网产业已经走过了不寻常的25年，深刻地影响着中国社会的各个方面，飞速地改变着我们的生产方式和生活方式。去年，我国在5G、量子通信、人工智能、云计算、大数据、区块链等领域都展示出强劲的发展实力。

随着5G时代、万物互联时代的到来，新形势下的安全问题也日益严峻。以5G为例，移动通信实现了海量互联，用户体验数据率提升了10倍，频谱效率提升了3倍，5G不仅比4G更快，它支持的业务类型更多，应用范围更广。5G的安全是双刃剑，一方面，5G实现了计算与通信的融合，基于大数据、人工智能的网络运维，减少了人为的差错，智能化的监控有利于提高网络的安全防御水平。另一方面，由于5G的虚拟化和软件定义能力以及协议的互联网化、开放化，也带来了新的安全风险，使网络有可能遭到更多的渗透和攻击。

我们在为5G欢欣鼓舞的同时，也必须正视5G带来的安全挑战。以5G为依托，被大家看作是互联网发展下一方向的工业互联网，也同样面临着极大的安全威胁，工业互联网的发展模糊了物理世界和虚拟世界的界限，由此引发的网络攻击往往会造成比过去更严重的影响。在刚刚过去的7月，我们看到澳大利亚、美国等国家的一些城市都相继出现了大面积断网停电的重大事故。越来越多的事实表明，安全威胁已经从网络空间蔓延到大型制造、电力、交通、医疗等现代社会的命脉行业中，而且这些行业无不关系到国家的稳定和群众的利益，因此工业互联网需要采取更为严格的安全防范技术。工业互联网的安全需要管理与技术发展并重，企业的安全要与行业的安全、社会的安全结合，实现威胁情报共享与协同联动。工业互联网24小时永远在线，让工业互联网的安全工作永远在路上。如何实现共创共享，网络信息安全企业、政府部门、运营商互相形成大数据协同，获得实时威胁情报和风险通报及解决方案，利用外部力量帮助企业提升工业互联网的安全防御，这都是工业互联网亟待解决的核心问题。

互联网的安全问题是国际化的问题，需要加强国际合作，维护全球共同的互联网安全生态。网络安全已经是国家、社会、企业乃至个人绕不开的重要命题，需要各个领域以及每个个体携手共建互联网安全大生态，发展网络安全行业是当务之急。我们期待国内外网络安全知名企业、中小企业和业内专家共同围绕网络安全政策与法规、工业互联网安全、城市安全、5G安全、漏洞挖掘、网络安全人才培养等重要议题，分享先进经验，碰撞新的思想，共同建立网络安全的大生态。

360集团董事长兼CEO周鸿祎：

网络战没有平时和战时之分

本报记者 李佳师

> 网络安全对人类经济与社会的威胁很大，无论什么样的国家都面临网络安全的挑战，所以全球应该在网络安全方面携手交流，共同应对网络战对人类命运共同体的威胁。

360集团董事长兼CEO周鸿祎在第七届互联网安全大会上表示，必须用作战的视角看待网络安全。网络战最大的特点是不宣而战，对手会花相当长的时间通过攻击手段进行攻击和潜伏，渗透到对方的基础设施网络里，在关键时刻给对手致命一击。这意味着，潜伏渗透本身也是网络攻击的一部分，所以网络战没有平时和战时之分。

周鸿祎在演讲中表示，网络战不是科幻小说或者美国大片里幻想的未来，网络战就发生在当下，每天都在发生，乌克兰电网遭攻击、伊朗遭遇震网病毒都是活生生的例子。所以我们必须意识到网络战的严峻形势，如果像将头埋在沙子里的鸵鸟一样不承认网络战的存在，不能意识到网络战带来的挑战，根本谈不上应对网络战，过去所有在数字空间里的打击都可以转成物理世界的伤害。为什么网络战现在越来越受到关注，因为现在所有的网络战攻击目的不仅仅是为了窃取情报，而是有可能对交通、能源、金融等基础设施发起攻击，关键基础设施已经成为网络战的未来战场。

周鸿祎进一步表示，很多人、很多公司都在兜售和传播这样的观点，认为买了技术、系统之后就可以保证网络安全，就可以高枕无忧，这其实是谎言。因为今天所有的网络攻击之所以能得手，其实是利用了不知道的漏洞。事实上，所有软件硬件都是人做的，是人做的就有可能存在漏洞、存在缺陷。每1000行代码里通常会有4~6个错误，试想，今天那么多的自动化系统、云计算、大数据、人工智能中有多少代码，这其中隐藏多少漏洞。因为有漏洞，网络战部队就有可能攻进来。而且网络战是整体战，即便最后的目标是攻击一个国家的基础设施，也往往是从攻击一个人开始的。以个人为跳板，攻击这个人经常上的网站、经常用的邮箱，经过一连串的攻击链，最后到达基础设施。所以在网络战里是不分国家、企业和个人的，安全是一个整体。

周鸿祎认为，应对网络战，“看见”是关键。事实上，最可怕的是别人来了你不知道，别人走了你也不知道。如果不能解决“看见”网络攻击的问题，堆砌再多的网络“军火”和网络产品都没有意义。而网络安全大数据是“看见”的基础，因为网络安全大数据可以记录整个网络空间里所有正常软件的通信行为和不正常的行为，只有在各种维度上把全网所有发生的事情看清，才能真正知道网络空间里发生了什么。所以，网络安全大数据需要全网数据，既包括企业，也包括消费者。此外，威胁情报和知识库是构建AI大数据的前提。有了大数据和知识库之后，网络战的本质就成了人与人的对抗。高级别的攻防专家会在最后关头起到决定性作用。

周鸿祎最后表示，网络安全问题对人类经济与社会的威胁很大，无论什么样的国家都面临网络安全的挑战，所以全球应该在网络安全方面携手交流，共同应对网络战对人类命运共同体的威胁。

新加坡网络安全专员、网络安全局首席执行官许智贤：

采用四大战略应对互联网安全威胁

本报记者 李佳师

> 新加坡在推动网络安全的国际合作上有三种方式，一是推动国际组织讨论关键网络问题。二是召开东盟部长级会议。三是充分利用务实的合作，推动区域能力建设，共同建立网络安全领域。

新加坡网络安全专员、网络安全局首席执行官许智贤（David Koh）日前在第七届互联网安全大会上指出，网络安全已经成为未来数字经济及智慧城市的关键部分。应对安全挑战，我们需要共同合作建立安全的网络安全关系和生态环境。

许智贤表示，新加坡在2017年、2018年时遇到很多网络安全的威胁，占犯罪比例的20%。在这样的威胁下，政府和利益相关者意识到，要加大国家网络安全政策制定力度，优化网络安全生态系统。2016年起，新加坡网络安全局以四个网络安全战略应对网络威胁。

第一个战略是建立有弹性的基础设施。保障网络基础设施是提高核心服务的主要部分，使重要部门在网络攻击的环境下受到保护。新加坡去年颁布了《网络安全法案》，法案强调关键基础设施的网络安全防护。法案中要求对基础设施的业主责任进行认定，需要对网络安全措施进行再评估以及审查自己的基础设施，并且将网络事件报告给网络安全局。法案要求网络安全部门响应任何网络安全事故调查。

第二个战略是创建一个安全的网络空间。要确保电力公司和公民有网络安全意识，也希望企业和公民能够意识到网络安全的重要性。在推动强有力的数字经济发展的同时，公民、设备、网络、企业绝对不能暴露在风险中。

第三个战略是建立充满活力的网络安全系统。新加坡政府希望网络安全行业不断增长，给人们提供更高附加值的工作以及更好的就业机会。为了实现这一目的，现在我们正吸引世界顶级网络安全公司来新加坡运营，并且建立分公司。

第四个战略是加强国际合作，共同应对跨国网络威胁。网络空间和传统陆海空空间没有太大区别，都要遵守世界贸易组织建立的贸易规则。

现在全球许多国家都在利用人工智能、大数据等技术，未来我们的生活、工作将越来越依赖于数据空间。因此，我们要明确建立和制定并实施网络空间的规则，把规则应用在生活和工作中。

为实现这个目标，联合国召集一系列国家政府专家共同探讨安全措施。目前，新加坡在推动网络安全的国际合作上有三种方式：一是推动国际组织讨论关键网络问题。二是召开东盟部长级会议。三是充分利用务实的合作，推动区域能力建设，共同建立网络安全领域。

以色列国家信息安全局前局长埃雷兹·科雷尔：

网络安全是个系统工程

本报记者 李佳师

> 目前，无论是卫星系统，还是国家的银行、水、电力、污水排水、通信等系统，都非常容易受到黑客攻击。我们今天面临的安全挑战越来越严峻，一旦这些领域出现安全威胁或问题，就会造成整个国家崩盘或是关键基础设施崩塌。

以色列国家信息安全局前局长、以色列国家网络安全委员会前主任埃雷兹·科雷尔在第七届互联网安全大会上以《以色列网络空间安全国防体系建设思路》为题作了演讲。

埃雷兹·科雷尔在演讲中表示：“当我们思考交通运输问题的时候，要考虑其安全性。而网络也是运输体系中非常重要的一部分，网络使得这些交通运输体系可以更好地运行。如果你坐在车里面，突然听到来自系统的声音说‘你好，我刚刚劫持了你的汽车，如果你不给我四个比特币，你的家人和你自己是无法刹车的’，试想遇到这样的情况，你会怎么样？我们都不希望这样的事情发生，所以，必须做好计划，以应对这些可能出现的情况。”

埃雷兹·科雷尔表示，目前，无论是卫星系统，还是国家的银行、水、电力、污水排水、通信等系统，都非常容易受到黑客攻击。我们今天面临的安全挑战越来越严峻，一旦这些领域出现安全威胁或问题，就会造成整个国家崩盘或是关键基础设施崩塌，对手不需要射出一颗子弹，就可以使整个国家系统瘫痪。

埃雷兹·科雷尔认为，我们今天面临的安全挑战之所以严峻，一部分原因是由于在基础设施当中有很多旧的系统，古老的基础设施系统与复杂的IT系统连接在一起时，就会出现很多漏洞。网络攻击并不是一种标准化的攻击，这些网络武器的“火力”无法测量，病毒没有身高、没有体重，但它可以和指挥台、导弹一样产生战略性的后果，而且网络病毒有很多的分支。发射几千枚导弹很难，但是要传播几百个、几千个恶意病毒却很容易。

目前在以色列有500多个网络安全初创企业。“在过去的5年当中我走访了很多初创企业，见到了很多创新性的公司和很好的网络安全创意。以色列和中国相比，有点像小船和航母，小船无法做航母所做的事情，但可以快速穿梭，很灵活。”埃雷兹·科雷尔说，因为我们没有这么多的人力资源，所以很多东西需要自动化，需要非常创新的解决方案。比如当我们考虑互联网医疗的时候，包括远程医疗、远程手术、远程医疗辅助等，就需要同时将网络安全系统考虑进去。因此，从这个角度说，网络安全是一个系统工程，需要进行快速应对，所以我们应该携起手来。

硬件木马威胁严重 检测技术成为关键

工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）
翟腾 高宏玲 郭青帅

信息技术的发展极大地促进了社会的进步，但同时信息的泄露也严重威胁到了个人、公司乃至整个国家的安全，为了保证数据信息的保密性，必要时要对数据进行加密处理。

伴随着解密技术的进步以及数据重要性的增加，数据安全面临着严峻挑战，原有的加密手段存在的安全风险越来越大，迫切需要新的更安全的加密技术。正式发布于2001年的高级加密标准（Advanced Encryption Standard，AES）作为传统对称加密算法标准DES的替代者，以其灵活、高效、安全、可靠等优点，成为众多行业部门的密码标准。

数据经过AES加密算法加密后，恶意攻击者即使获得了密文信息，在无密钥的情况下想要获取有效的明文信息也是十分困难的。对于这类加密应用场景，获取密钥信息成了一种较为普遍的选择，在加密模块中植入硬件木马已成为一种有效、可行的重要攻击手段。硬件木马是恶意攻击者在硬件产品的设计、制造或二次开发过程中，出于某种特殊目的人为制造的非法模块。硬件木马的植入使得电路中预留了能够绕过硬件加密壁垒，通常电路都能够实现预期的功能，因此并不容易被发现。硬件木马攻击能够影响大量的器件，并且检测困难，因此，硬件木马被认为是对所有安全模型的一个重大威胁。

FPGA广泛应用于通信以及图像处理等多个领域中，为了防止数据通信过程中信息的泄露，通常在数据发送前进行AES加密处理。由于FPGA的开发特性，导致其开发使用过程中很容易被植入硬件木马，通过修改原始逻辑结构，将加密过程所用到的密钥信息发送至外部，被攻击者所接受，从而达到破解密文获取明文信息的目的。

正因为硬件木马带来严重的威胁，因此，对于电路中硬件木马的检测成为一项重要的研究内容。国外的一些高校、企业和科研机构，针对硬件木马检测技术方面的研究开展得相对较早。IBM Thomas J. Watson研究中心、伍斯特理工学院、德国波鸿IT安全研究中心、Intel公司、新墨西哥大学、耶鲁大学、康涅狄格州立大学、加拿大海军研究院、美国Phoenix Technologies公司等机构和企业都陆续加入到硬件木马的研究中来。而国内对硬件木马的研究起步较晚，直到2010年年底才有关于硬件木马设计的文章发表，部分高校、研究院等都陆续开展了关于硬件木马检测方法的研究。所以，对于国内来说，硬件木马及其检测技术的研究是一个崭新的领域，还处于起步阶段，研究广度和研究深度都很有限。因此，有必要深入研究硬件木马检测技术，完善我国在硬件安全性和完整性领域的技术研究体系。

硬件木马设计灵活，隐蔽性强，并且植入简单，给硬件木马的检测带了严峻的考验，同时也对检测设备的灵敏性以及数据处理、分析方法提出了更高的要求。

为了检测电路中是否存在硬件木马，一些检测方法相继被提出来。其中基于旁路信号分析的检测方法成为硬件木马检测的主流方法，也是效果最好的检测方法。旁路信号指在硬件模块工作过程中产生的功率信号、时序信息、电磁信号、热量等敏感信息。硬件在工作过程中都会发出各种不同的旁路信号，不同的器件其自身的组成结构、工作方式决定其旁路信号都是确定的。如果原始模块中被植入了硬件木马，各种旁路信号都会受到木马的影响从而出现变化。所以，我们可以收集、测试待测模块的旁路信号，再与原始电路的旁路信号进行分析、对比，根据对比结果判断电路中是否存在硬件木马，这样的检测方法被称为基于旁路分析的硬件木马检测技术。目前最常用的主要是依靠分析功耗信息和时序信息来检测硬件木马。通过电流探针等测试设备，对被测模块功耗变化进行测量，并对测试结果进行降噪、降维等处理，求解二者电路的功耗信息之间的相关性，根据相关性大小做出是否被植入木马判别。该方法对于占用资源较多以及功耗较大的木马电路，有着较高的检测成功率。

社长：卢山 社址：北京市海淀区紫竹院路66号赛迪大厦18层 邮编：100048 每周二、五出版 周二8版 周五8版 零售4.50元 全年定价420元（包含手机客户端） 广告部：010-88558848/8808 发行部：010-88558777 京昌工商广登字第20170004号 经济日报印刷厂印刷