会议时间：2018年5月12日14：00-17：46

会议地点：悠谷一期4楼P444会议室

会议主题：网络空间安全论坛

李洪涛：尊敬的各位领导、各位来宾、媒体朋友们，大家下午好。5月的南京繁花似锦，气侯宜人，今天我们相聚在这里参加“第二届全球未来网络发展峰会（网络空间安全论坛”。我们共同探讨当前热点和未来发展新趋势、新理念，分享网络空间安全技术与产业发展的真知卓见。对于贯彻网络强国战略和网络安全信息化事业发展，具有非常重要的意义。

接下来，由我来介绍今天参会的各位领导和嘉宾，他们是：

本场论坛主席、国家互联网信息办公室信息发展局副局长、中国互联网络信息中心副主任曾宇

江苏省未来网络创新研究院常务副院长谭航

中国电信股份有限公司云计算分公司总经理胡志强

国家互联网应急中心副主任兼总工程师云晓春

国家工业信息安全发展研究中心副主任、副所长李新社

杭州安恒信息技术股份有限公司首席安全官、高级副总裁刘志乐

中国互联网络信息中心主任助理胡安磊

国家信息中心安全管理处处长、高级工程师邵国安

中国信息通信研究院安全研究所所长魏亮

绿盟科技副总裁宫智

还有来自媒体界的各位朋友们，再次向各位领导和嘉宾的到来表示热烈地欢迎！

下面，首先有请中央网信办信息化发展局副局长、中国互联网络信息中心副主任曾宇致辞，大家欢迎。

曾宇：尊敬的各位来宾，大家下午好。很高兴与大家相聚在美丽的古都金陵，共同就网络安全相关问题做研讨交流。我首先代表网络空间安全论坛的承办方（英文）向在座各位表示热烈地欢迎！并向本届全球未来网络发展峰会主办方表示衷心地感谢！

党的十八大以来，以习近平同志为核心的党中央坚持从发展中国特色社会主义，实现中华民族伟大复兴中国梦的战略高度，举旗定向，谋篇布局，全面推进网络安全和信息化工作，网信事业取得了历史性变革和成就。

当前，我国互联网发展迅猛，根据（英文）第四十一次报告同时显示，截止到2017年年底，我国网民规模达到7.72亿，普及率达到55.8%。互联网各项新技术、新应用层出不穷。与此同时，我们要清醒地认识到我们面临的网络安全形势也日益紧张，网络安全威胁和风险日渐凸显，以及被社会各领域渗透。全球范围内的网络安全态势可谓暗流涌动。

习近平总书记强调，网络安全和信息化是两翼，必须统一谋划、统一部署、统一推进、统一实施。要以安全保发展，以发展促安全。俗话说：“聪者听于无声，明者见于无形”，我们作为网信战线的排头兵、主力军，更要全方面对网络安全做好工作。面对当前诸如APP泄漏攻击等等，我们对威胁隐患做到心中有数，我们要清楚地认识到网络安全威胁具有很强的隐蔽性、欺骗性和破坏力。一个技术漏洞安全风险可能会很长时间没有发现，一出问题具有极大地杀伤力和影响力。

习近平同志强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。为此，我们也要清楚地认识到风险在哪里，是什么样的风险，什么时候发生风险。在网络安全中，我们要掌握我们的主动权。我们必须深入研究采取有效的措施，切实从方方面面来着手好网络安全，来土地我们网络安全相关技术和产能工作。

所以今天我们承办这个论坛，也是希望和我们产业界、学术界、专家朋友们一起，我们把网络安全相关技术和产业现状、趋势，以及可能存在的风险和问题，我们做深入阐述。所以也感谢主办方提供这样的平台，一个思想碰撞交流的平台、一个合作的交流。

所以维护网络安全一是我们要树立正确的网络安全观，要落实习近平总书记的重要讲话，与习近平总书记网络强国战略思维为统领，提高政治站位，增强行动自觉，切实把思想和行动统一在总书记重要讲话精神上来。二是加强核心技术和新技术的科研攻关。我们提早部署，及早攻坚，有了核心技术才能不断增强我国网络安全防御能力和相关的防御我们外部攻击的能力。三是加强对未来网络新应用的预判，研究其对传统安全防护体系带来的历史性机遇与颠覆式挑战，提早做好部署应对，确保在共享未来网络发展红利的同时来做到网络安全局面切实可控。

网络安全为人民、靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织共同参与。今天我们举办“网络空间安全论坛”就是要集大家之力，听大家之言及共同为我国网络安全事业发展贡献力量。你们的思想观点、意见建议对于推动网络安全工作意义非凡，共同就网络安全当前的热点问题、未来发展的新趋势、新理念，技术与产业发展，发表我们的真知卓见，在这里碰撞出智慧的火花。

最后，衷心地预祝本次论坛取得圆满成功，谢谢大家。

李洪涛：非常感谢曾局长的致辞。

下面，有请江苏省未来网络创新研究院常务副院长谭航致辞，大家欢迎。

谭航：尊敬的各位领导、各位专家、各位朋友们，下午好。初夏时节逢盛会，五月的江宁气侯宜人。昨天在未来网络小镇刚刚迎来“第二届全球未来网络发展峰会”的开幕，今天在微风细雨中各位嘉宾集聚一起就，网络空间进行研讨与交流，我谨代表峰会承办方之一的江苏省未来网络创新研究院，欢迎各位领导、专家和嘉宾的到来，也衷心感谢论坛演讲嘉宾即将给我们带来的思想分享，也衷心感谢论坛承办方国家互联网信息中心领导们，对峰会及论坛的支持。

网络空间涵盖互联网相关的通讯网、计算机系统、自动化控制系统、数字设备，及其承载的应用与服务，及数据等多种元素。它正全面地改变着人们的生产和生活方式，影响着人类发展的历史进程。网络空间是我们信息传输的新渠道，生产生活的新空间，经济发展的新引擎，文化繁荣的新载体，社会治理的新平台，合作交流的新纽带，也是我们国家主权的新疆域。但网络信息技术的广泛应用和网络空间的信息发展，在极大地促进经济繁荣和社会进步的同时，也给我们带来了新的安全风险与挑战。

网络空间从建设到应用无时无刻不面临着网络渗透、网络攻击、网络有害信息的传播、网络恐怖及犯罪活动，这对我们的网络空间安全从管理到治理均提出了新的要求和新的挑战。根据习总书记网络强国的战略思想，4月20日召开的全国网络安全和信息化工作会议，对网络空间安全工作也提出了新的要求。我们今天的论坛也是对总书记思想和网信工作会议要求的进一步贯彻落实，我们就网络空间安全从建设、应用、管理和治理之道上进行研讨，从技术体系、应用安全、管理保障及产业等方面展开交流，探索相关的趋势，研究相关的理念。

我相信，论坛各位专家领导精彩的演讲和无私的分享，一定会为我们带来新的视野和新思维，便为我国网络空间安全工作的进一步推进提供有益的建议和智慧。

最后，我祝愿本次论坛取得圆满成功，祝各位领导、专家和嘉宾们身体健康、工作顺利，也希望来自外地、来自远方的朋友们抽空再来未来网络小镇、多来未来网络小镇，谢谢大家。

李洪涛：感谢谭院长的致辞。

接下来是报告解读时间。首先有请中国电信股份有限公司云计算分公司总经理胡志强，演讲的主题为“助力企业上云：从技术、标准和生态打造安全云”。

胡志强：尊敬的曾局长、各位来宾，大家下午好。非常高兴参加“网络空间安全论坛”，我借这个机会向各位来宾好好地学习，同时也介绍一下中国电信我们在网络信息安全方面，这些年来我们做的一些工作。特别是在天翼云中国电信云计算领域，我们中国电信在这方面做的一些工作，请各位领导和专家批评指正。

放眼全球，这些年来我们信息技术日新月异，我们的网络事业发展在我们中国也可以说是突飞猛进。但是与之伴随的就是网络信息安全面临着日益严峻的挑战。为此，我们从国家层面对这个问题高度重视。在2016年11月份，全国人大颁布了《中华人民共和国网络安全法》，将网络安全等级保护制度上升为国家法律，意义非常重大。在同年12月份，国家网信办发布了《国家网络空间安全战略》，这是我们国家首次向全世界系统地、明确地展示和宣誓、阐述网络空间安全的主张，应该来说这个也是意义非常重大。

十八大以来，总书记在网络信息安全发表了一系列的讲话，清晰地描述了网络强国的战略思想，提出了没有网络安全就没有国家安全，就没有经济社会的稳定运行，这个是总书记在4月20-21日在全国网络安全和信息化工作会议上的一个重要的讲话。作为中国电信来说，我们作为我们国家基础的网络信息运营商，怎么样来贯彻总书记讲话的精神？把总书记的讲话落实到中国电信的各个方面工作实际当中去，怎么把网络工作安全、网络信息安全抓落实抓到位，就要求我们加强信息基础设施的安全防护、加强网络安全信息统筹机制、手段、平台建设，加强网络信息安全应急事件处理，防患于未然，要落实关键信息基础设施的防护责任，严厉打击网络黑客、电信网络诈骗、侵犯公民隐私等等违法犯罪的行为，维护人民的合法权益。这方面，作为中国电信我们责任重大、任重道远。

从信息技术来说，我们从CT时代到IT时代，到现在的DT时代，伴随着我们技术的进步，我们的网络信息安全面临着不同的挑战。我们在传统的CT时代，我们的电话语音和端到端的传送怎么保证安全。到的计算机时代，我们动态的数据信息在计算机网络中怎么样可靠地传输，怎么样保证不被篡改，保证正确的接收，这是我们面临的一个新挑战。

到了现在随着移动互联网、大数据、云计算、IOT技术飞速发展，我们面临着新挑战，那么就是CT技术、IT技术、DT技术融合，互相交织带来了新的更复杂的安全问题，这是我们面临的非常大的挑战。另一方面，核心技术、关键产品受制于人。刚才曾主任也讲了，最近我们闹得纷纷扬扬的，中美贸易战引发的新片大战，我们关键的系统受到攻击的隐患，信息被窃取的风险，压力越来越大。作为我们信息通信技术产业的从业人员，我们确实面临着非常严峻的挑战。

从中国电信来看，我们是把网络安全作为中国电信健康发展的基石。我们现在正在推进三化转型，网络智能化、业务生态化、运营智慧化。我们战略转型的目的就是要为我们客户、为中国数字经济的转型提供信息化的服务能力、提供进一步增强信息化服务的能力。为了做到这一点，我们信息化服务的基础就是要网络信息安全保障。没有网信的安全就没有中国电信的安全，更没有中国电信健康的发展，这是我们中国电信的一个基本的理念。

当前，作为通信运营商，特别是中国电信我们面临着通信诈骗、信息泄露等等一系列新的安全问题，而且这些问题道高一尺，魔高一丈，而且成为全世界的焦点问题，三大运营商都是如此，名字叫做电信诈骗，对于我们中国电信是非常不利的。其实这个是我们整个行业的问题，我们现在跟全国人大相关机关沟通，看能不能把电信诈骗改一下，这个确实是我们现在面临的非常严峻的问题。为什么说网信安全是我们中国电信健康发展的根本保障，我们整个为了保障网信安全，我们中国电信构建了一个完整的网络与安全的体系，包括制度和能力建设，也包括了基础网络的安全，特别是包括了云的安全服务和数据安全的保障。

下面，我会从这几个方面一个一个地汇报。网络信息安全对中国电信如此重要，我们首先要做的就是要构建一套体系，中国电信网络安全制度和能力建设，包括组织体系、队伍建设、能力体系、规章制度。从组织体系来说，我们在2007年就成立了集团级的网络信息安全领导小组，由集团主要领导亲自挂帅。我们组建了集团和省两级网络信息安全的部门，这个是管理单位。我们还建立了网络和集团、省级两级操作中心，我们也设立了不良信息处理中心。从队伍建设来说，因为网络安全技术门槛比较高，需要专业化的人才队伍，所以我们建立了集团网络信息人才选拔基地制度，而且这些专家是享受人才津贴的。我们现在拥有网络安全专家77人，同时两级安全操作中心有数百人专业人才队伍，通过人才队伍来保障网络信息安全体系能够执行落地到位。从能力体系来看，我们构建了两大平台，一个是SOC平台，一个是信安平台，通过这两大平台的建设能够确保我们在技术能力上，能够保证我们的网络信息安全落实到位。同时，在国家监管层面我们能提供可靠的保障。像移动上网日志留存平台就是有要求的，我们中国电信专门构建了相应的平台，来满足监管部门合规性的要求。在规章制度方面，我们制定了完善的管理办法，规范开展安全管理和考核。包括网信安全基础信息管理、风险处置预案和风险网络安全事件闭环管理等等。通过一系列的安全制度和能力建设，保障中国电信网络安全、信息安全的管控到位。

这个是从中国电信网络监测DDos5年的情况，我们当前确确实实不容乐观，看看DDos的攻击。如果再看看5年我们会面临比这个更加严峻的局面，为了应对日益增加的网络攻击行为，中国电信举全集团之力自主研发了云堤产品，作为防范网络攻击行为的基础网络安全产品。包括四大类，抗DDos攻击、域名无忧、反钓鱼、网站安全专家。

网络安全基础服务和业内其他服务商，我们在产品和能力上到底有什么区别呢？我们云堤得益于中国电信运营着我们最大的互联网接入骨干网络，互联网的骨干网络和宽带的接入网络，中国电信是运营着这么一张大网络。得益于这一点，所以我们的云堤拥有国内最大规模的攻击防护能力。我们在全球部署了36个分布式清洗中心，从清洗能力来说，我们不仅可以做到进入目的地的清洗、近源的清洗，还可以针对高流量攻击提供高防的服务，将攻击流量引流，保证客户业务不间断的运行。我们提供PB级独享防护能力，客户零部署、零操作，非常方便。云堤这个产品，我们认为这是现在是具备国家队的能力。

从具体效果来看，中国电信作为央企、作为基础通信运营商，我们担负着国家重大任务的安全服务工作。从十九大到2017年两会、2018年两会、“一带一路”峰会、达沃斯论坛、金砖五国峰会等等一系列国家重大任务，中国电信我们的基础安全服务，我们在后台提供保障，特别是云堤的产品。所以我们说中国电信在基础网络安全服务方面，我们承担着国家队的角色，具备国家队的能力。

接下来，我想重点说一说我们在云计算领域，我们中国电信的解决方案。相对于我们传统的IT环境，应该来说在云的环境下，网络信息安全面临着更大的挑战。这里面CSA云安全联盟定义的12大类安全威胁，右边都列举了，包括了比如说云服务中数据库等资源、系统漏洞影响范围，怎么样防止从单击扩展到所有的多用户，这是我们面临很大的风险。比如说，我们怎么样来防止管理员权限过大，通过挂卷接触到用户的数据等等，这都是在我们的云的环境下面临的一些问题。在云的环境下，我们不仅面临传统的IT环境的安全问题，我们还面临虚拟化的环境、云管的平台等等，我们面临一系列安全风险防范的问题。

既然我们在云的服务环境下，我们的企业上云、政府上云、面临这么大的风险和压力，对安全这么关注，中国电信我们建立了一套整套云的整体安全体系，也是我们提供云安全服务的一些基础。那么，包括了安全的管理体系、技术体系、运营体系。安全的管理体系方面，我们包括了组织体系、策略体系，这方面是中国电信的强项。运营体系方面，我们中国电信在多年来，在通信网络运营维护方面我们经历了丰富的经验，具备了非常高可靠的电信级运维能力，所以在安全运营方面我们同样是如此。

在安全技术体系方面，由于云计算跟传统的IT环境不太一样，各家都有一些差异。我在这里分享一下我们中国电信的做法。中国电信我们在云安全服务方面就是要围绕怎么样实现业务和管理分离，能力与能力的区隔。通过两类网络来设计资源池的资源架构，一个是内部核心的网络，一个是外部核心的网络。内部的核心网络将所有内部子区域连接在一起，在整个网络中是安全的区域，并且是管理系统的核心。外部的核心网络，怎么样为互联网租户提供服务，通过安全设备连接互联网，所以这两个网络是隔离的。同时，我们划分多个服务区，整个网络分为多个服务区，实现不同功能及安全级别的设计。这是我们采取了针对性的策略，确保业务和管理的隔离，能力与能力的区隔。

另一方面，我们中国电信的云重点可能跟阿里、腾讯还不太一样，我们重点是面向政企客户提供安全的服务能力。在这种情况下，我们政企客户他不仅特别关注的一点是什么呢？尽管我们云的平台已经提供了相对安全的保障，但是他们更关注的是我们在共享资源的环境下怎么样来保证他们的安全。针对用户的关注点，中国电信在业内第一家首家推出了专属云，我们这个专属云提供三大类的服务，包括计算资源独享、计算存储资源独享、计算存储网络资源独享，为用户提供专属云的服务。这是第一个方面。

第二，在网络方面包括云资源池的互联，包括云资源池专线入云服务。我们的传统做法是用VPN的方式来解决这个问题，在中国电信为了应对用户对安全的关注，我们提供了专线的服务，包括云间高速提供QoS保障，包括了入云专线和传统的专线服务等级完全一致，就解决了用户关注的云间互联和入云连接的端到端的问题。这是专属云也好、云网互联也好，这是整个中国电信云计算独特差异化优势。中国电信我们是提供网络的，那么网络的安全、专线的能力是业界最高等级的安全保障。

目前，我们为我们的政企客户提供了从网络到平台到应用的全系列标准化安全服务产品，覆盖了政企客户对云安全TOP6的需求，右边我们列出了TOP6的需求。同时，我们安全的产品具有独特的一些优势和特点。比如说，我们的DDos防护是5G免费流量清洗，我们协同云堤提供T级防护能力，这是在业界其他云服务商目前做不到的。在WAF防护我们提供电信全网DNS秒级刷新，同时我们为政企客户提供电子化服务，包括渗透测试、包括漏洞扫描。

大家都知道，我们云这块的安全确实非常复杂。在云的环境下，怎么样确保提供安全的服务，光靠中国电信是不够的，我们一定要引入安全的生态合作伙伴打造合作共赢的生态圈。这一点呢，我们中国电信提供了天翼云、提供了云市场，为我们各个方面、各个行业的网络安全专家、网络信息安全专家，我们共同在这个平台上来为我们的客户提供整合的网络安全能力服务。在这一点上，中国电信完全是开放的态度。我们在下半年七八月份准备召开天翼云生态大会，邀请各位嘉宾关注，希望通过生态大会建立起天翼云，特别是云安全服务方面合作共赢的生态圈。

在云安全服务方面，还要特别强调的一点，因为企业上云也好、政府上云也好，要面对政府严格的监管。从用户角度来看，他们也要对云安全认证有非常迫切的需求。针对这个方面的需求，中国电信我们为200多家客户提供了安全等级保护三级认证。2018年，我们全部的资源池要具备中国电信天翼云资源池，全部要具备等保三级服务认证能力。我们现在在广州资源池具备了等保四级能力，这个是目前全国第一家通过等保四级云资源池。2018年中国电信正在做规划，对重点资源池进行等级保护四级认证，为我们金融行业的客户提供更加可靠、安全的云资源的能力。这七个方面我大概介绍了我们中国电信在天翼云、云安全服务方面我们具备了一些能力。

再一个就是数据，大家都很关注数据安全。数据安全到底靠什么？靠技术、靠管理，可能这些都很重要。但是中国电信认为用户的数据安全，最重要的是靠服务提供商的理念、靠你的操守、靠你对客户的承诺。中国电信承诺绝对不碰用户的数据、绝对不会利用用户的数据从事同业竞争的行为，这方面是中国电信作为央企我们多年来已经形成了非常好的口碑。

我们认为不管你有多么强大的技术手段，建立了多么强大的数据安全的防护机制，只有你真正做到承诺不触碰用户的数据，那才是真正的安全机制落实到位。这一点呢，我们中国电信切实履行我们的承诺。

网络信息安全确实是我们在面临不断变化的环境，我们会迎来各个方面新的挑战。在的环境下，比如说我们在云化这块云网不断融合。比如说在软件化环境下，我们会面临很多新的问题。比如说，我们现在信息安全工作主要是人和人之间的对抗，接下来如果是机器和人之间的对抗，我们怎么来应对？这个很快可能就会成为现实。比如说，我们现在物联网方兴未艾，传感层的安全如何来保障？僵尸网络是否会更加的隐蔽？这些问题都是未知的挑战。但不管怎么样变化，运营商是我们实现网络信息安全最底层的屏障，要提供最基础的防护能力，适应这种新变化。我们要迎接新的挑战，要保障新的安全，要提供安全可信的云网基础设施和融合服务，要为我们的国家网络信息安全做出我们应有的贡献。中国电信我们应该要承担起央企的职责，为我们国家网络信息化、网络信息安全做出我们应有的贡献。我们要提供安全可信的云网的融合服务，我们坚信我们一定能做到这一点。

我大概跟大家汇报这些内容，谢谢大家。

李洪涛：非常感谢胡总对我们的精彩报告。胡总分享介绍了中国电信落实国家网络安全战略，打造安全可信的云网环境的探索与实践，分享了宝贵经验。

下面，有请国家互联网应急中心副主任兼总工程师云晓春，演讲的主题为“2017年我国互联网网络安全态势”。

云晓春：尊敬的曾局长、各位领导、各位专家，大家下午好。非常荣幸我能参加今天的这个论坛，今天我就想主要是向各位汇报一下我们国家互联网应急中心，对于2017年我们国家互联网网络安全态势的一个认识。

我们说在2017年，我们国家对互联网网络安全总体态势应该还是不错的。我们互联网网络产业发展非常迅猛，网络安全产业也快速发展，空间也进入了一个法治的新时代。但是同时面临的网络安全问题也日益复杂。

根据中国互联网信息中心报告，2017年我们国家网民规模达到了7.72亿，现在我们可以说是互联网规模是稳居全球第一的。而且在2017年的时候，我们网络安全产业发展也非常好，国内的企业整体规模达到了400亿，同比增长了33%。特别是大家都知道去年是十九大的召开之年，在十九大报告中总书记报告专门提出来，提出网络安全是我们人类面临的许多共同挑战之一，也就是说把网络安全提升到前所未有的高度。在去年，我们在实际的生产生活中发现了大量的网络安全问题，各种网络安全问题日益错综复杂。

在这样大的背景下，我今天主要介绍三个方面的内容。首先，给大家介绍一下利用我们自己的技术平台对于我们国家2017年互联网络安全一些监测数据。主要是从六个方面进行介绍。首先，恶意程序方面。对于针对计算机的恶意程序，我们2017年发现境外控制服务器大约有3.2万个，同时发现境内感染计算机恶意程序达到1256万台，实际上跟前几年相比一直呈现下降的趋势。也就是说较2016年下降了26.1%，总的来说这几年是呈现下降趋势的。感染计算机恶意程序中，远程控制木马的数量最多，达到了71.65%，僵尸网络木马占比20.3%。

在感染计算机恶意程序所形成的僵尸网络中，超过1000台达到了855个。因为我们现在一直跟主管部门的领导下，每个月都要定期对互联网上僵尸木马程序进行清理，来保证互联网上网络安全的环境。在去年，我们一共治理了664个控制规模较大的僵尸网络。在去年，我们发现新的恶意程序253万个，较前年增长了23.4%。在这里主要就是三类移动互联网恶意程序，包括流氓行为类、恶意扣费类，以及资费消耗类。我们在去年累计向92家国内提供移动应有程序通报了移动互联网恶意事件，下降了8634个。

在联网智能设备恶意程序方面，我们发现去年控制规模超过1000台的僵尸网络发现了343个。在这里面，最大规模5万台也发现了有5个。而且就是说，这些被恶意程序控制的智能设备主要是有12种恶意代码的家族，这是下面列出来的12个恶意代码家族。

在安全漏洞方面，因为我们中心成立了一个国家信息安全漏洞共享平台，我们是国内最大规模的国家级漏洞库。我们收录了通用软硬件漏洞15955个，同比上涨了47.4%。收录的漏洞里面涉及到谷歌产品的漏洞是最多的，达到了1133个，占整个ZNVD全部收录漏洞的7.1%。同时我们在漏洞库中建立了4个子漏洞库，包括移动互联网子漏洞库、电信行业的子漏洞库、电子政务的子漏洞库等等，我们涉及到政府机构等等事件达到了26892个，同比增长10.9%。在安全漏洞方面，联网智能设备安全漏洞去年增长非常快，在2017年我们所收录的联网智能设备安全漏洞达到了2440个，同比增长118.4%。涉及到的产品包括家用路由器、网络摄像头、会议系统，这些漏洞类型包括了命令执行、文件上传等等。

第三类安全事件就是拒绝服务攻击。在去年总主要的监测发现三类，一个是TCP，再就是NTP反射放大攻击，再就是SSDP反射放大攻击。反射放大攻击中的主要流量是来自于境外，我们对攻击进行分析发现有一个非常大的特点，发起攻击的次数呈现密集分布的特点，实际上是少量攻击资源发起攻击次数。我们去年发现21个控制端全年连续6个月发起攻击，去年发现3万多个，但实际上有21个控制端有连续6个月发起攻击。有271个肉鸡地址全年连续8个月都被利用发起攻击，101个反射服务器全年连续8个月连续被利用发起攻击。这是我们做的示意图。

在网站安全方面，去年一共监测发现仿冒页面4.9万个，下降72.5%。全年共协调处理页面2.5万个，涉及移动互联网的页面7000多个。被植入后门的网站数量2.9万个，同比下降64.6%。涉及IP地址约2.4万个，90.6%位于境外。在网页篡改方面，我们发现境内被篡改网站2万个，同比上涨20%。被篡改政府网站有618个，同比上涨32.3%。

工业互联网的安全，国家在推动网络强国战略的时候，工业互联网也是作为一个网络强国战略中非常重要的方面。我们在去年监测发现，我们国家工业互联网面临非常大的潜在威胁。包括我们发现了200例左右联网公众设备或者平台存在着严重的漏洞隐患，发现在我们互联网上有4772个设备是曝露在互联网上。我们在去年监测境外IP地址对境内联网工控设备245万次扫描。

现在国家在大力推“互联网+”行动计划，其中互联网金融已经汇集了我们国家的方方面面，我们中心也是建立了相应的互联网金融分析平台，对国家互联网安全进行宏观监测。2017年抽取1000家互联网金融网站进行安全评估监测，发现了严重的用户数据泄露风险。

下面，简单地给大家介绍一下我们综合的判断，在2017年国家互联网网络安全的状况。我们国家在2017年互联网络安全状况呈现了比较显著的特点。

第一，我们国家在网络空间法治进程迈入新阶段，2017年6月1日《网络安全法》正式实施了，可以说是我们从去年6月1日开始进入了一个全新的网络空间法治的新时代。

第二，我们国家在网络反诈工作持续推进。2016年出现了一系列电信诈骗的情况，所以到了2017年的时候网络反诈作为重要工作推进。在2017年的时候，全年共协调处置仿冒网站2.5万个，域名境外占比44.9%，同比上升了14.2%，有88.2%位于境外。

第三，网络武器库泄露后的风险威胁日益显现。大家知道在2016年、2017年的时候，（英文）组织在2017年的时候把NSA网络武器公布出来了，其中有一个就是针对微软“永恒之蓝”的攻击程序。这种非常专业的，像CIA、NSA非常专业的部门研发出来的网络安全武器泄露出来之后，黑客会马上拿过来用，这样的风险非常大，一下子门槛就给降低了。

第四，敲诈勒索和挖矿等牟利恶意攻击事件数量大幅增长。我们在2017年的时候新增捕获勒索软件近4万个，呈现快速增长趋势。在2017年下半年的时候，数字货币价值暴涨，这就导致了针对数字货币网络安全事件频发。大家知道去年5月份病毒勒索的就是B2B，以及用于“挖矿”的恶意程序数量大幅上升，并推动了区块链技术的大热。

第五，应用软件供应链安全问题触发连锁反应。在2015年9月份的时候，当时被曝露出来的就是苹果的开发工具被植入XcodeGhost恶意代码，只要用这个来开发APP都会有恶意代码，这是很威胁的。到2017年的时候又出现了一系列应用软件供应链问题，还有内置问题等等，这个现在看来供应链的安全会成为一个很大的安全问题。当然了，今年中兴事件更是体现出供应链安全重大的问题。

最后，给各位介绍一下我们认为在2018年，我们需要在网络安全方面关注的一些热点问题。第一，对于个人信息和重要数据保护方面会变得非常重要。因为在国内一个比较大的教训就是2017年3月份的时候，公安机关破获了一起盗卖公民信息的特大案件，犯罪团伙涉嫌入侵社交、游戏、视频直播等等重要信息50亿条。在今年的时候欧盟推出了GDPR，也就是一般性的个人数据保护的法规。在这里给全世界的公司提出了非常大的挑战，在它的GDPR里面明确规定，我们一般意义上认为做隐私保护的时候往往都是保护国内的，保护的就是中国公民在中国国内的数据是要受到保护的。但是在GDPR里明确提出了，只要是欧盟的公民，即使他在中国，他的数据你也是不能随便进行获取的。整个从这个态势上来看，全世界各国对于公民隐私保护提到了前所未有的高度。我们国家也一样，将来怎么样进一步细化立法这方面的问题。

第二，我们认为在2018年的时候安全漏洞信息保护将会成为非常重要的问题。因为漏洞本身现在是被大家认为是一个国家的战略性资源，每一年我们也都会发现大量的各种新的漏洞。在这种情况下，漏洞到底按照什么样的方法来披露，这会成为一个很重要的问题。《网络安全法》26条规定，向社会公布系统漏洞应当遵循国家有关规定。没有原则的往外公布，可能最后对厂商也好、对企业也好，包括对个人也好都会造成很大的危害，甚至可能危害国家的安全。所以说到底怎么样来进行漏洞的信息保护、披露，这在今年会成为非常重要的问题。

第三，物联网设备面临着网络安全威胁加剧。现在万物互联，现在越来越多的物联网呈现在我们的家庭和生活中。2017年的时候，我们CNVD收录的物联网社一安全漏洞数量较上年增长近1.2倍，2017年每日活跃的受控物联网设备IP地址达2.7万个。去年下半年的时候两办推出了关于推进IPv6的行动计划，包括大力推动5G。当IPV6和5G推动，我们相信会大大增快物联网发展。当物联网设备越来越多的时候，它的安全问题会变得越来越明显。

第四，数字货币会引发越来越多的更复杂的网络攻击。现在像B2B等等数字货币不断呈现，在我们国家给打出去了，不允许在国内使了，但是在国际上还是有使用的现象。现在针对各个不同的平台上推出了专门平台的挖矿木马，所以在今年我们认为数字货币的安全问题也会成为一个热点的问题。

第五，我们认为在2018年应该关注的就是人工智能运用在网络安全领域的热度会持续上升。现在只要搞IT的可能张口闭口都是人工智能，确实是能解决很多的问题。人工智能在网络安全的热度不只是用在防范，攻防和两方面都会用。黑客利用人工智能技术来突破网络防御，防护者是关心怎么样用好防御人工智能技术。所以在攻防方面怎么用好人工智能将成为一个非常重要的，在今后相当长一段时间内都会成为人工智能安全领域非常重要的问题。

以上我给各位汇报了一下我们对于2017年网络安全态势分析的情况，不当之处请各位领导和专家指正，谢谢大家。

李洪涛：感谢云主任的精彩报告。

下面，有请国家工业信息安全发展研究中心副主任李新社，演讲的主题为“对工业信息安全问题的探讨”。

李新社：各位与会的代表、专家，大家下午好。在这里和大家探讨一下工业信息安全的问题。先给大家讲几个概念，第一，工业信息安全和工业互联网的关系。我们现在谈工业互联网，实际上网络空间是一个很大的范畴，这个范畴把工业互联网和工业信息安全的内容包含在里面了。我们过去没有网络这个概念的时候，一谈工业都是那种封闭的、比较小的或者是一个大工厂没有连网的状态，我们把它称之为传统的工业状态。

今天，我们把它变成一个大的网络的时候就变成新的东西了。这时候我们就讲工业信息安全已经成为一个重大的问题，这个重大问题体现在两个方面，第一，传统工业时期，企业尤其是生产制造业各干各的，没有连网。即便是自己企业内部也没有那么大的信息系统。近10年以来，尤其是近20年以来由于计算机的快速发展、信息化的快速发展、信息化技术的快速应用，所有传统企业，尤其是在我们国家，我们国家又是一个工业基础、工业门类非常完善的一个国家，从材料、制造什么地方我们几乎都有，包括市场我们也存在。所以这个时候传统工业搭上了信息化快车的时候，我们天天讲两化融合以后，传统工业往前走了一步，过去讲自动化、自动控制。再往前走一步因为有了互联网，所有的传统企业驾驭在互联网上跑的时候，安全又成为一个新的特点，这个安全就是工业互联网的安全。

那么，工业互联网的安全在工业信息安全中间又是一个其中的门类或者说一个部分。现代工业没有互联网大家都知道没法干事，但是正是因为有了工业、有了互联网，尤其是现代工业有了互联网之后，又给现代工业的发展带来了新的挑战和新的安全隐患。大家知道，当一个封闭系统在一起做的时候，你根本对外都不打开，你也不上互联网。如果想捣乱破坏的话只有一件事，翻墙进你的大门把你的机器整坏。当工业控制系统拎到一张网上的时候，当这张网又在互联网上溜达的时候，我可以不翻墙进你的工厂，刚才国家安全应急中心的同志也介绍的一下关于网络的问题。其实远程控制、远程入侵，这个时候就出现了。

我不知道在座的有多少人看过以前的电影，七八十年代的电影讲到工厂的时候，那时候非得进你的大门把看门老头打晕了以后搞破坏。今天当我们把计算机技术应用在工厂的机器上，当我们把工业控制系统应用在我们的生产机器上的时候，这样一个过去传统的工业企业所面临的问题就呈现了新的状态。这个状态我把它叫做工业互联网面临的大的问题，也就是工业信息安全面临的大的问题。

国旗就是工控安全，现在已经变成了工控安全、工业互联网安全，现在已经占了非常大的比重。

现在谈一下工业互联网的认识和相关主要的问题。这张图告诉大家大致的工业互联网构成是这些内容，比如说平台、应用软件、供应商、操作系统等等，每一个环节都有可能出现问题。从保障对象的角度来看四大类，工业数据、平台运营商、网络基础设施、工业企业。基础网络我就不说了，我们现在天天讲的网络安全，你脑子里面呈现的大致是基础网络那部分。但是对于工业数据安全、平台运营商安全、工业企业的安全，这三个方面我们如何看待它的问题？可以这么讲，这么多年以来，尤其是近五年以来，尤其是近来三年以来，中国的工业体系更加完善、中国的工业发展更加快速，但是我们大多数处于工业环境中的这些人，因为大部分的人是老的工业体系下培养出来的人，对于工业信息安全的概念在脑子里面很多人没有形成。

这两天到南京，在南京碰了几个大学的教授，聊天的时候说到了一件事情，某大学利用第三方的软件开发了一个平台，实际上是一个办公平台。这个平台被发现有漏洞，这个人就问我说你们单位是搞安全的，这个要紧不要紧？我说你第一时间赶紧让第三方把漏洞堵了。这个事情可能会产生两个问题，第一，你不堵这个漏洞，假设这个漏洞被人侵犯了，把页面篡改了，你们领导要承担主要责任。第二，一旦这个漏洞被曝光是某某公司开发的什么平台，那个公司损失巨大。在这个话题之外，我所感受到的一个重大的就是这些大学教授也是一个科技大学的领导，他对这个概念还没有那么强烈。我们深处这个环境中，因为有一些东西我们所监测全国、全世界的这些事我就不跟大家说了。我清清楚楚地知道这个中间的危害有多大，这是非常严重的一件事情。但是就我们在言谈话语中间，这些大学教授对这个事的概念很小。当然这包括我们到一些企业去调研的时候，你跟企业领导讲，你们的那个软件漏洞怎么样、你们的工业控制系统用的什么控制系统等等。我可以不夸张地讲，当前我们国家，包括世界上的一些国家运用的工业控制系统中的那个控制的部分，无一例外都有问题。有的问题大一点，有的问题小一点，有的问题容易发现，有的问题可能要经过高级的那些人员折腾才能看见，基本上是这样的状态。所以我在这里先强调一下工业控制系统，工业信息安全的这个问题一定、务必、必须让大家重视起来。否则在我们国家这么快速的发展状态下，尤其是今天我们面临这么错综复杂的国际问题，中国全面的工业基础都这么好，一旦这个问题不重视，它要进来全面给你搞瘫痪的时候，你那时候哭都来不及。虽然我们国家在网络应用、物联网、云计算、大数据等等这些方面的应用，在全球运用比较多，某些方面还是比较领先的。但是这种领先不表明你的安全在全球就是比较牛的，这是两回事。

有几个问题跟大家分享一下。第一个问题，2017年以来，我们中心监测了很多的漏洞。大家看这张图有一部分工业安全的漏洞相当多，这还是2017年的，到现在变化非常大。我们所监测的更多的是偏重在工业系统安全里面，这也是我们国家的一个命脉，任何一个大国如果没有工业基础，你想成为全球领先的大国，这事不大可能。这些问题很多东西，你像PRC，我们那个时代做PRC芯片的时候，基本上会借助计算机或者是一台仪器把数据烧进去，而且烧进去之后不可更改。但是我现在告诉你，PRC的入侵基本上可以不用计算机，由一个PRC直接发起攻击到另外一个PRC，只要你在网络上有联络，就直接可以进去，非常可怕，而且这种漏洞我们已经验证过了。

第二个问题，公共平台。我们现在开发的所有公共平台，我和南京教授聊天的时候他们是第三方开发的，第三方开发的平台我问你，你有没有问他，他经过什么样的安全检测软件进行过检测。一周以前也是在南京讨论的另外一个话题，我跟美国的一个互联网联盟的秘书长，他说了一件事，他说他希望能够推动一件事情，这件事情就是当你的软件开发出来之后应该用一个第三方的可靠、认可的工具来进行攻击和检测，看你这个软件和平台的安全性和可靠性到底怎么样。我相信，我们在座的如果你是搞开发的，我相信你们开发的时候一定是本着如何完成甲方给你的要求，把这个程序编得非常漂亮，界面弄得非常好看，本着这个思想的。你的第一出发点绝没有含安全方面的事，甲方说你把这个东西给我做出来，比如说姓名、性别，这些随时可改，这些要求流程上你做得非常棒。但是，你做完之后交给甲方，甲方上线运行的时候只是看这个软件能不能按照我的这个流程从第一到第十能不能干下来。我们从来没有去想某一个坏蛋、某一个黑客在暗地里说你一上线我有没有偷你的东西。我真的希望我们的软件上线之前，包括硬件在内的这些系统上线之前应该经过某一个专业的工具进行测试。比如说，你的内部的一张表格，表格中间填的有文字、有字母、有数字，还有别的一些信息。你有没有用一个软件进行破坏性的测试，填乱七八糟的东西，看填到什么时候是不是崩溃。在座的各位到工厂去参观或者是调研的时候，你会发现我们包括手机在的这些产品出来卖之前要经过各式各样的检测，有些检测比如说有温度的检测、压力的检测等等一大堆的检测。可是我问你，我们编的一个平台软件、编的一个系统软件，你经过这一类跟工业有点类似的这种检测吗？这是当前我们认识的重大误区，而且这个误区如果不重视，将来出现的问题可能会更大。

前段时间，我们讨论的时候我举的例子就是电梯控制的例子。我知道有一些电梯在全国卖电梯的时候就在中间植入一些传感器，他会说你这个电梯用了10年、8年，哪个零件容易出问题，我就帮你来修。殊不知，这种零件在互联网上传数据的时候很可能被人截获，被截获之后可以远程控制你的电梯上下。假设这部电梯装在某个非常重要的地方，这个电梯又被人控制了，当国家领导人或者某个重要的事情在这个电梯中间要发生的时候，电梯失控出问题，你想想这种危害是多大，这个事情是存在的，被电梯控制的事情是存在的，因为我们发现过漏洞

第三个问题，大数据安全的问题。我认为是两个方面的事，第一，产生数据是不是安全的。大家知道，我们的某一个工业控制平台不一定是完全没有漏洞的，不一定是一个没被人控制的。你这台系统产生数据的时候，那个数据真的就是那些东西吗？这是第一个问题。第二，即便产生的时候非常多，所有的系统产生的数据都是对的。传输过程中传到中央控制器或者云端的时候，这个过程如果有人进来把你的数据改了，你的数据还安全吗。所以现在大家一谈大数据，没有太多人说大数据安全概念是什么。你去医院检查，化验一滴血的时候拿错了可能出来的数据就错了。化验过程中机器出了问题没有校准，产生的数据给你的数据也不对。这就是这个过程中间出现的问题。

所以我们在讲数据采集、数据存储，在进入数据挖掘的时候，当数据采集过程当中是对的，存的时候存错了，挖的时候肯定挖不对，挖出来对的话如果在输出的时候出了时候被感染也是问题。我们在检验监测过程中发现有一类数据是非常麻烦的，我没法判断你这个数据到底是真的还是假的，有没有错，我没法判断这件事情。家用传感器、摄像头，只要在网上跑，因为你那个摄像头就是连视频的网，只要在网上跑有可能发现漏洞以后，你这个数据传的时候可能都有问题。我只是告诫大家，脑子里面一定要有那根弦，当你做开发者或者你是第三方检验机构对数据进行检验检测的时候，安全要放在最头上。早期人家编程序的时候就会说用什么样的数据是比较安全的，用什么语句编这个程序是不错的，用什么不行。当你编程序用数据库、用别的时候东西的时候，你得想假设那个人是个黑客要进来的时候，你采用的这条语句会不会被人用走。

接下来给大家谈一下工业信息安全的态势。习总书记多次强调，包括今年4月20日又一次强调网络安全的问题。这个中间比较复杂的一个重大的问题是网络安全主权的问题，欧盟你再牛，说你的公民跑到中国来他的信息数据也不能用在中国来，这个事情产生法律冲突。大家记住，一个老外在中国犯罪他一定会适应中国的法律，因为你在我的国土上。网络空间安全，习总书记在2012年的时候提出网络空间主权的时候，西方国家坚决反对，为什么？习总书记讲，网络空间的主权也是国家主权的一部分，是国家主权的一个延伸，这是中国提出来的鲜明的观点。换个角度看，西方国家别想用网络来控制我，我认为这件事情是推动人类命运共同体建设中间的一个重大的理论创造发明，应该是这个角度去看。网络空间主权，你只要在我的国家你别废话，你都得听我的，你不能在网络上胡说八道就不行，应该是这样的概念。你进入我们这个国家，你在我们这个国家采购发生的一些跟网络数据有关系的问题，我们国家按照我的国家的法律应该有权处理，按照欧盟的法律你无权，这是绝对的对抗，这些事情在现实中间都存在了。

从安全演进路径讲，工业信息安全已经成为国家安全体系的有机组成部分。过去封闭系统的时候，工业安全信息提的并不多，现在不是这样了，我不用翻墙进去我就能搞定你。我们工厂的这个网络物理全是隔离的，物理隔绝的网络在远程射屏的干扰下是可以入侵的。汽车咱们现在不用开钥匙了，走到车门口一拉就开了，是一个蓝牙短程通讯系统。这样一个系统几年前已经发现漏洞了，你那个系统我根本不要你在不在跟前，我远程可以把车开走。这个在《速度与激情8》电影里面特别典型，他说的那个事在现实世界中是存在的，只不过大家没见过发生的就是了。这是一个简单的讲说物理隔离是不是就怎么着，一个是远程的无线入侵。第二，你自己在内部没有把握好用了不该用的光盘，其他的一些系统只要插到你的系统中，这个系统可能就成为一个定时炸弹，只不过没有激发的点。一旦激发那个点成熟，你的整个系统会崩溃的。我们物理隔离系统是不是就牛的不得了，别人就进不来？也不见得。

第二，从全球范围来看，工业信息安全形势日趋严峻。美国是世界老大，他的问题比较多，技术也比较强。我们是新兴国家，我们在发展过程中对安全问题的考虑并不周到，所以这里面的隐患非常多。比较典型的刚才云主任谈的，给你公布一堆漏洞，有些人就用这个漏洞。3月份北京市海淀区信息被披露的事，就是一个中学生干的，用了第三方工具下载之后开始入侵一大堆网络，那些网络的脆弱性真是不忍直视，直接进去把数据偷出来就卖钱去了。我们有一大堆的网站系统安全上的不堪一击。

第三，从国家的角度来讲，战略布局是任何一个国家，尤其是发达国家特别重视的一个点。我们国家也无一例外，我们2016年发布战略，2017年发布《网络安全法》，6月1日开始实施。这件事情在我们国家的网络生活中是一个重大的事件，《网络安全法》的颁布。为此我们中心做了全国巡回《网络安全法》普及工作，我也去了好几个地方，东南西北都去过。但是每到一个地方你会发现工业基础高低、网络发达和不发达之间，他们对《网络安全法》的认识差距巨大。我们过去容易讲发达地区是东西差距、南北差距等等。从网络角度来讲，网络安全意识差距也非常大。有些人你跟他讲网络安全，他觉得这事跟我远着呢，其实一点都不远。

从技术发展角度来讲，开展工业系统安全应急演练，我们叫工业靶场，现在做得比较多，美国做得比咱们要多很多，刚才公布的那些东西很多都是美国自己干的。做一个靶场去攻，然后看哪里有问题。去年11月份我们组织了一个全国网络演练，在杭州。我们中心组织全国网络演练的时候来了东西南北，最终进入决赛的是50支队伍。第一，拿了一些防火墙或者是一些系统把这个队伍分成两组，你先来发现漏洞，拿出来的这些系统和这些东西有一些企业觉得我的系统非常牢固，基本上说想进来不容易。但是通过半天的时间，交卷的时候发现这套体系或者这个防火墙漏洞百出。一方面，显示我们国家IT人才水平很高；另一方面，说明我们当时在研究防火墙或者系统的时候，这些企业安全上的考虑可能考虑了，但是不是完善的。第一步完了，发现漏洞之后怎么办？你再负责把它堵上。堵上以后呢，接下来的比赛就是交换系统，你不是把系统的漏洞都堵完了吗？交给另外一波，但是仍然发现漏洞。可以这么讲，我们国家从技术上来讲不是说有些技术做不到，只是说当前工业系统安全、工业信息安全从这个角度来看问题还是比较大的，只是我们每一个人都非常善良，非常善良地认为我们的工业系统别人不是要进来的，是如何利用它给老百姓生产更好的东西的。但是别忘了，有黑天就有白天，有光明就有黑暗，任何一个很好的事物出现的时候总有一些利益集团或者是有别的目的的机构，他会对你产生一些别的想法。所以从这来讲，我想利用这样的论坛告诉大家，如果你在从事工业信息安全、工业信息系统开发这方面工作的话，安全问题务必要放在头等重要的位置上。

第四，从我国现状来讲，工业信息安全的风险逐步威胁到经济社会健康发展。因为我们国家是一个工业门类比较全的或者是最全的国家，我们拥有全世界最大的国内市场。当有人在你这个系统中间渗入了漏洞、木马、后门的话，对你有一些想法的时候，这个威胁就大了。自来水系统、水库，这是跟我们生活密切相关的，还有电。我们过去的水库找俩工人搬轮子把闸抬起来，三峡大坝你抬起来试试。你只要有计算机、通信系统，安全隐患就存在了。所以目前看起来，我们所监测到的问题和发现的问题可以这么讲，工业信息安全的风险确确实实逐步地会影响到我们国家经济的健康发展，这也不是耸人听闻。所以在未来的几年，尤其是2025完成以后，接下来的发展我们安全问题恐怕要上升到另外一个更高的高度上去。

接下来跟大家谈一下我们面临的安全挑战。首先是社会意识不强烈、企业意识不强烈、个人意识不强烈，这三个问题同时存在。而且社会意识、企业意识、个人意识在很多人眼中基本上是没有的，就是安全意识是没有的，这是我们当前面临的重大问题。不均衡的问题我就不多说了。

另外一个方面，我们目前的安全系统处于起步阶段，核心的内容、核心的技术等等受制于人，这是我们面临当前最大的现状。所以接下来我们要做更大的努力，核心技术赶紧弄到手，赶紧开发我们自己的体系。当然，这种开发不是封闭的开发，我们要掌握这种核心体系。

坚持国家的总体安全观，这是习近平同志告诉我们的话，要以“本质安全、内外兼顾、业务优先、隐私可控”为安全保障原则。你发起的这个系统或者研发这个东西本质上是安全的，要从这个角度来考虑。

最后和大家简单说一下我们的对策，第一，认识到安全的问题是一直存在的，要认识到这个问题。当然，还要组建工业信息安全的国家队，要把它的能力打造起来。我们中心去年3月21日，从原来的工作重心转移到以工业信息安全为重心的点上来以后，我们把大部分的工作都往这个方向在转。一方面是两化融合，要大力推进；另一方面，信息安全也要进一步挖掘中间的内容。要做好20个方面的关键措施，这些我就不在这里多重复了。这些不一定说20个够不够，有些人说我这些都做得差不多了。我们现在在靶场、系统安全、漏洞验证等等在做这方面的工作，我们的工作也是起步状态，国内的这些工作基本上处于一个大的起步状态，跟欧美发达国家相比我们确确实实，尤其是跟美国相比还是有差距的。这有赖于我们在座所有的人在这方面要进一步的努力，发挥自己的才智，把我们国家的工作能做好。

简单说两句，3-5年工业信息安全市场会进入一个快速的增长期。如果你的企业是干这件事情的，把安全的东西多弄一点，把核心技术多开发一点，要掌握核心技术，这是我们的命根子。第二，要实现全覆盖。我们过去的安全系统只是对工厂、企业、传统企业说的事，现在智能化以后，智能化所有的设备都要植入工业信息安全的大概念，才有可能在未来的发展过程中不出现重大的问题。第三，新机遇。如果你是干这个的，投资也好、做工作也好，这方面机遇很多，也可能是接下来的一个发展非常快速的产业。第四，产业化、集聚化、协同化难度比较大。

简单跟大家汇报这么多。但是我跟大家讲，工业信息安全将来一定会跟我们的生活密切相关，而且不是一般的相关，是一个强相关的关系，谢谢各位。

李洪涛：感谢李主任的精彩报告。

下面，有请杭州安恒信息技术股份有限公司高级副总裁、首席安全官刘志乐，大家掌声有请。

刘志乐：各位领导、各位专家，下午好。非常有幸在这边跟大家一起分享一下，在新时代下我们安恒在网络安全方面的一些思考。

最近有一个名词比较热——数字经济。数字经济也包括了互联网、工业互联网、大数据、人工智能等等。但是我们这些技术怎么样能更好地服务人们、服务社会，需要安全作为它的保障，所以需要这些产业和安全进行融合。

我今天跟大家分享的第一个关键词就是融合。在不久之前，我们跟中国比较知名的一家做物联网设备视频的探头，我们做了一个技术上的融合。我们把我们安全的技术融入到他们的摄像头里面，叫做安全育苗。有了这样的技术，这个摄像头曝露在外面的时候自身就会有安全免疫能力，而不会像之前我们所听到的说出了什么样的一些问题。在下个月，在杭州的一个区里面就会部署带有安全育苗的摄像头。

除了刚才说的这种，还有我们在城市治理方面，我们的线上、线下的这种融合。我们也知道，现在城市整个的治理，包括了传统的一些智慧政务，包括现在有了更多的一些云计算等等，这些都会跟我们日常的生活息息相关。我们把这些所有的数据，现在有的讲是城市整个治理中心，有的讲叫城市大了。我们怎么样把我们所看到的所有的威胁感知和整个安全大脑的决策，怎么样把它互相的结合起来，最终能是一个相当于实现一个决策。在整个城市治理当中，我们把我们整个的情报和我们的大脑，然后最后到整个的应急处置决策，然后实现城市治理当中的线上线下的融合。

除了城市治理方面，刚才就像李主任说到的工业互联网。工业互联网也跟我们人们的生活越来越相关，作为工业互联网现在整个在网上它的一些统计，在这个地方我就不多说了。但是实际上，最近如果大家关注国际形势的话，实际上美国他们现在已经很明确，他说要把打击对方的关键基础设施的这种能力作为他未来重要的战略。所以在这个时候，我们怎么样来保证我们的工业互联网的安全就愈发显得非常重要。所以刚才李主任也说了，他们去年专门成立了国家工业互联网安全中心，从国家的高度对我们整个工业互联网进行总体的安全设计。在我们过去也发现很多关于工业互联网方面的一些安全的问题，今天时间的关系，我就不在这边做更多的赘述。

除了刚才说了城市治理的融合、工业互联网的融合，还有我们AI与安全的融合，这个也是最近这两年比较火的一个话题，人工智能怎么样跟安全来做一个有效的融合。之前我们听到更多的人工智能说是阿尔法GO，但是阿尔法GO更多处理的是结构化的问题，但我们真正的网络安全里面更多的要处理的是属于非结构化的问题。可喜的是，我们这两年在这方面也加大了大量的投入，我们把多元的数据存储起来，通过我们的阿尔法大数据智能的安全分析加上相当于无监管自动的、自学习的模型来进行快速的安全威胁的响应和处置，能够实现发现异常、发现变化、降低误报。

我们现在的处理能力、检测的时间MITD可以提高20X，MTIR响应时间可以提高19，误报率可以降低500%。这是在AI方面，不是说人工智能就会减少我们对于网络安全人才的需求。恰恰相反，我们有了人工智能之后我们更加需要专业的网络安全的人才。结合人工智能和安全专家，最终可以给出一个最佳的安全解决方案。

最近还有一件事情也比较热，就是数据安全与隐私保护的新挑战。facebook损失惨重，最新欧盟也推出了世界上第一个对于数据保护的GDPR。在数据保护这一块，更多的我们要做到我们的数据我做主，要把数据还给用户、还给老百姓。

在这些方面，我们要思考怎么样相当于把我们的数据放在一个安全屋里面，在这个安全屋里面怎么样能做到刚才我们所说的，我的数据我做主。尤其是在中国，我们的数据更多的是根本没有经过我们的同意就被无线地使用，或者是被售卖。所以通过这些技术手段，我们可以去实现你的数据是在一个安全屋里面是被使用了，而不是被他过度的使用。可以做到可监控、可追溯、可用不可见，以及最小化的原则。

再一个就是，我们在拥抱互联网的时候，实际上一些犯罪分子他们也在拥抱互联网，他们利用现在最新的互联网技术来对我们实现精准的诈骗。针对这种情况，我们在一年多前相关的监管部门找到我们，让我们来通过技术手段怎么样来去帮他们能快速地发现和打击这些诈骗的犯罪团伙。可喜的是，通过我们的技术手段实现以网治网，来实现监管部门新的监管手段，来打击网上违法的诈骗行为。我们去年做的已经被部里面作为示范的工程，我们来创造真正清朗的网络空间，以促进发展更多的双创萌芽。同时，态势感知对物联网的新监管，我们也做了更多的一些融合。我刚才给大家汇报的是前面融合的方面。

第二个汇报的关键词是赋能。我们怎么样把传统的或者说也算是创新的网络安全公司，这么十多年的网络安全专业的能力来赋能给所有需要的行业和部门。在上个月的20日，习主席召开了最新的今年网信工作领导小组的工作会议。在这个会上，首先他也提出是两年前提出来没有网络安全就没有国家安全。同时他今年提出来，核心技术是国之重器，最关键、最核心的技术要立足于自主创新、自立自强。所以我们作为做网络安全的，我们要知己知彼，我们要快速发现攻击，我们要有主动的攻击。知己就是我们要自我感知和自我防御能力。

我们通过从需求到研发、到测试、到上线、到运营，然后形成不断迭代的循环来实现知己知彼，安全的赋能。说到知己知彼，我们在过去的这些年，比如说2017年6月份，我们在一个边疆的系统里面发现了一个APD行为，而这个事件后来通过我们跟主管机关一起最后来确认，这个潜伏的事件长达8年之久，这就是一个知己知彼的过程。通过我们的能力去发现了APD的攻击行为。同时，我们前面几位专家也说到了，现在整个曝露在互联网上的，比如是去年类似于美国国家安全局武器泄露，整个造成勒索病毒，之前是“永恒之蓝”是SMB的端口。我们通过我们自己的系统可以发现，比如说在中国被植入后面的组机感染数是20055个，占全球数量的22%。这个是当时发现勒索病毒的时候，我们的阿尔法大数据实验室第一时间通过大数据技术对全球整个受感染情况，做了一个统计，我们及时汇报给主管部门。

刚才也说到了，核心技术是国之重器。我们现在在做的这种类似于导弹头一样的，这种核心的全网检测能力，我们对于全球整个检测一次，整个测绘的能力仅需要两个小时，而且我们还具有全球的准实时的监测能力。这是我们整个发现的一些数据。之前一段时间，ckco爆发了设备上的一个漏洞，它在已经修补的情况下，我们又迅速地去检查一次，还发现全球还有超过6万台设备还存在着ckco漏洞的影响。

还有就是连接的赋能。通过我们的能力加上我们的赋能，然后来连接更多的行业而实现我们的能力赋能给这些行业。

还有人才的赋能。我们最近在做一件很有意义的事情，在今天西湖论剑上我们做了一个发布，我们内部把它叫做X计划，实际上就是学习的计划。我们在中间把安恒、实训和认证、产业合作伙伴进行对接。当学生走入社会的时候，除了拿到学校的毕业证，他还可以拿到一些认证，而且跟产业可以迅速融入到产业里面。我们也做了一个三年的计划，我们三年要和100家培训机构，和1000所高校合作，培养10万名网络安全的工程师。

最后跟大家分享的是共创。面对现在这样的一个非常严峻的网络空间环境，肯定不可能是我们比如说安恒一家或者不可能是哪一家就可以把网络安全方面的问题都能够解决。我们需要跟工业互联网安全研究中心等等，包括我们要跟行业里面所有的一些其他的网络安全企业，包括一些比如刚才讲的中国电信甲方企业，我们要一起联合共创，相互来启发、来创新，以实现我们应对当前整个网络安全复杂情况。

今天在智慧城市里面，它的安全治理和建设越来越显示出共创，把整个智慧城市的治理和建设能够做得更好。在前面，我们在有些地方已经在做着这样的一些实践，包括像上海整个城市的态势感知，实际上更多的是一种大家共创的结果。

我今天的汇报就到这里，谢谢大家。

李洪涛：谢谢刘总的分享。

接下来茶歇10分钟，我们在4：10分开始论坛的下半场，谢谢大家。

（茶歇）

李洪涛：接下来，首先有请国家信息中心安全管理处处长邵国安，演讲的主题为“网络安全理念及态势感知平台建设”。

邵国安：各位领导、各位来宾，下午好。很高兴，一个是感谢CNNIC的邀请，感谢大会组委会让我有机会分享一下我自己在做网络安全，以及做态势感知平台建设当中的一些体会，提一些想法和理念。为什么讲理念？习大大说的，2016年习大大这个话讲完以后，你看两年多了，我们到底有多少在做了？比如说理念决定行动，前面几位嘉宾都说安全是发展的前提，2016年都提出来了。那就意味着你在考虑发展、考虑应用的时候，你必须首先考虑安全问题，这是在任何前提下都应该这么来做。

比如说我们讲全天候、全方位的感知网络安全态势。比如我们讲网络安全全方位，你包括哪几个方位，比如说我把网络安全做完了，网络安全包括哪几个维度。我觉得我们现在在这方面回答这些问题和做这方面思考的人不太多。既然领导已经说了这些，那是不是我们应该做，我们应该怎么做？怎么落地？这是我们要考虑的。王阳明有一句话叫知而不行，只是未知。好像很多看的都懂，但是你做起来的时候还是不懂。这样子，我就想把自己的思考给大家分享一下。

网络安全到底是什么？本质到底是什么意思？从网络安全的核心应该从哪几个方面来考虑？这些问题我们考虑的都不是太多，实际上大多数的都没有从本质上面来考虑。比如说我们讲网络安全的特点，比如说实效性、复杂性、专业性不对称。你遭到攻击的时候要马上处理的，这种实效性要体会出来的。你怎么发现攻击行为并马上处理，这是我们体现出来的能力，那种对抗。实际上能力的背后或者我们讲我们对抗的背后是一种什么样子？

所以我们讲做安全的话，一定是一个国家组织和个人的智力博弈的场所。你在做安全的时候，你永远不知道你的对手什么时间、什么时候用什么方式来对你发起攻击。在这种情况下，我们应该怎么来做？我们的对手是什么？我们的对手都是有国家、有组织背景的这些专业的人士，这种专业性就特别强。所以在这种过程当中，我们在做网络安全防护的时候我们应该怎么办？你怎么来提高你的网络安全防御的能力，来提高你的对手对你攻击的成本，我们应该怎么做。基于这样子，我的观点就是网络安全的核心实际上很少有人在研究，我感觉非常遗憾，我还是属于比较小众，大多数的观点还不一定被人接受但是你们自己可以判断我讲得对还是不对，我是从另外一个角度来考虑，然后给大家做一些参考。我认为网络安全今后要做的，一个是专业的分析队伍，第二个就是情报共享。不展开说了。

全天候是365天，7×24小时那叫全天候。我们大多数的安全厂商都属于卖盒子的，什么意思？就是说你买一个电脑你如果不坏，你永远不找他们，这就是盒子。如果你把安全当成一项服务，那7×24小时需要看到的。比如说防火墙，防火墙策略实时的监测有没有效果，有没有对于我做了安全策略他所采取的一些措施，比如说我把端口关了，有没有人对我进行探测，那是谁在探测，这是不是安全应该做的。所以说这里面我的观点就是改变观念，你怎么把你的基于对抗的理念放到行动上。在这种情况下，情报的共享是不是也可以特别重要？比如说我负责国家电子政务网络，我在北京发现的攻击和特征如果不共享出来，我自己处理完就完了，可能过两天在南京、杭州同样的情况会同样发展。所以在这种情况下，那就没有情报的共享、没有专业人员队伍的支撑，你这个安全是做不好的，这是我的体会。

在这种情况下，我们想到底应该怎么来做？这是一种理念。这是美国在CNAP上提出的要求，第一，实践证明单个机构已经没有办法应对复杂的威胁。第二，美国现在的做法是不再让单个的联邦政府来做单个的自己的IT运维建设和管理。但是我们国家的理念是什么？我讲出来你们都知道，我们的理念还是2003年中办的文件叫谁主管谁负责，谁使用谁负责。这种理念下的安全你怎么做。所以讲网络空间整个的系统关键及时、安全及时，实际上是需要研究人员、开发者、管理者、用户共同承担，所以这是一个。

苏格拉底有一句话，我们在座各位讲的网络安全跟我脑子里的网络安全一定是不一样的，那你怎么办那你就要术语定义。所以苏格拉底有一句话叫“智慧源于对术语的定义”。但是你看我们国家除了我们的标准，国家标准有一个章节叫术语和定义，其他所有的文件，包括技术文件都没有对术语定义这一说法。我们到现在是指导思想，这是不是有问题？你怎么来定义。我现在给我们部委、给省里面做方案、做技术文档的时候，我专门有一章节——术语定义。这是我的一种工作方法，如果这样子，基本上在统一的一个术语下面去讨论的话，你才会讨论很清晰。

不管电子政务、不管管控系统，在信息化网络安全，我们讲的习大大说的全方位。我是从五个方面来表现出来，你们认为是不是这么回事，你们可以自己判断。实际上你一分解，我的观点是复杂问题是要分解，而不是简单化或者是眉毛胡子一把抓。你一分解完，你会发现我们很多网络安全有问题。比如网络边界的安全，什么叫网络边界？国家关键基础设施的网络和互联网的连接点或者讲结合点，这是网络边界的安全，这是我的观点，到现在整体缺失。美国有TIC，我们国家是没有的。

第二，网络安全。我讲的网络安全更多的是基于动态的、行为的网络安全监控管理。你如果细想一下，我们的网络安全现基于等级保护、合规、基于静态的网络安全在做。

第三，终端安全。我们国家到现在对终端安全没有一个定义，你的脑子里面一会儿是服务器安全，一会儿是终端安全。笔记本电脑、台式机这些PC极端，还要包括可穿戴设备等等，更应该包括物联网前端设备，这是终端安全要干的事。终端安全可以分两类，一个是跟人关联的，你要把设备跟人绑定，证明这台设备是你本人在使用。物联网的安全终端，比如说公共系统，比如说更多的城市应急或者各个领域里面的物联网现在越来越多。那物联网的安全你是不是应该要做，保证设备传输出去的数据是你这台设备，那应该怎么做？数据的物联网芯片的安全、物联网在传输过程当中的安全，以及设备认证。

第四，应用安全。我们国家应用安全做得很糟糕，我定义的应该是基于单位身份角色的认证，以及应用软件原代码的安全和服务器的安全，应该叫主机安全，服务器裸机加操作系统。

第五，数据安全。你从采集到传输、到使用、到存储、到销毁，这是数据安全要干的事。数据安全要做数据的分类，原数据标准规范的制定，以及加密存储。

整个你把五个维度的安全如果都考虑到了，你的安全会做得比较好。但是你去看大多数都没有这样来做，你一分解，复杂问题就分解。你去看电子政务一直在讲电子政务的顶层设计，到底是什么样的顶层设计？我们讲了20年还在讲顶层设计。我理解的顶层设计，一个是顶层是对于电子政务的战略目标和规划的制定，从上往下。设计是什么？设计是从下往上的方案实施、工程实施以及落地落实。这样你的工程和实施是向你的目标去走的，我们没有，我们都是一个点一个点的工作。整个五个维度才是全方位整个的安全。

在这个情况下，这种安全的威胁既来自外部网络的攻击，又有来自内部的对于数据的窃取，所以整个数据在使用过程当中的全过程可控制、可管理、可追溯是不是我们应该考虑的。在座的有运维单位、甲方、乙方、厂商，你在做产品的时候是不是应该从这几个维度考虑。我如果是甲方我一定要提这样的要求，基于动态的安全从这五个维度一定要提，这样才能做得好。

我们为什么要讲这种明确的界定，就是智慧源于对术语的定义，这里术语实际上显得非常重要，国家这块太缺乏。现在让我来做，我就从基础工作做起。在统一的安全的概念和定义下面形成一致的认证框架，是你做好网络安全的基础。没有这个基础，我们现在都属于空中楼阁。我们讲概念和术语的挑战，实际上美国在布鲁金斯学会2012年就提出了《网络安全与美中关系》，网络安全领域定义中国人和美国人是不一样的。在国际上争取话语权，如果你定义术语都不一样，你怎么来做后面话语权的事情。

比如说美国政府有政府使用的术语定语，美国国防部有对国防部军事专业术语，包括欧盟相关术语的专业词汇和定语，这是人家国家这么干的，你看我们有吗。所以我多提一些问题引发大家的一些思考。因为刚才几位专家都已经说了去年的5·12，今天刚好是，想哭（音）病毒原因是什么？那是部分武器在互联网上面曝光，是不是全球的黑客都在研究这些网络武器库。对我们做防御的来说，是不是我们面临的挑战更大，所以网络武器库曝光以后，只要对我攻击了都认为是我的对手，他在研究这些网络武器以后，在我们网络里面的感知能力、隐藏能力、作战能力、行动能力都在增强，对我们做防御的是不是巨大的挑战，这种挑战我们准备好了吗？所以实际上多问几个为什么，我觉得我们的问题真的很大。

随便举个例子，因为这个是2015年炒的很火的，就是美国的认识管理局，400多万联邦成员信息被中国黑客窃取了。去年8月份到美国去开会去了，开完会直接被FBI带走，这就是起诉书。美国人怎么知道的？我们反过来，我们能不能够发现美国、俄罗斯各个全球的这些黑客对我们国家党政军网络的攻击，我们能指向他一个人吗？我们有这样的技术能力吗？基于对抗的背后是技术的展现和人才的展现。这就是中兴的，这个就不多说了。

我的观点就是说，态势感知平台到底怎么来解？这两年网上已经炒的很火热了，我的观点基本上都看不上眼。我的理念，一个是在互联网上面有两句或者讲必须牢记的原则。一个是你一旦成为目标，你总会是目标。这里面就有很多的案例，比如说东南亚的黑客度我们国家海洋安全持续的关注，你这两天处理完了，过两天人家会再来，持续对你的关注。比如说安全公司在研究全球到底有多少个黑客组织，他的每个黑客组织的特征是什么样子的，我们大概就能举起来几个，其实有很多。不知己知彼，你怎么做安全，这是一个。

第二，你必须放进来的，你就无法进行阻拦。比如说你的门户网站、邮件，你是必须开放到互联网上面的。所以为什么我们全球90%的APT攻击通过邮件，可以通过你的社会工程学、上下左右领导都可以确定目标，才能来进行攻击。基于这样子，我们应该怎么来做？这个是我们现在准备做的一个，就是对于事件的分级分类，我们国家现在没有的。所有的安全事件眉毛胡子一把抓，你怎么来分？比如说网信办、公安部天天对你的网站进行检测，发现漏洞就给你发个通知。那么在互联网上面跟黑客攻击的特征是一样的，你怎么区别出来？第二，比如说你发现了异常的行为，比如说我们经常发现电子政务的数据天天往美国、台湾、香港发，你该不该预警，我们讲跨境异常数据传输。还有更多的一些事件，你不分类你怎么去处理，你都不知道哪些是重点，哪些不是重点。下一步我们可能会申请国家标准，关于安全事件的分级分类或者安全事件报告的分级分类，国家是有分级分类的国家标准，但是那个事件的分级分类你看可操作吗？第二，他是指已经形成的安全事件的分类。如果没有形成的呢，比如说对邮件的暴力破解没有形成危害，被安全设备阻断掉的该不该分类。

基于这样的理念，态势感知还是从定义术语开始做。有效数据的获取，你们认为IDS的数据是有效数据吗？我们现在讲的（英文）系统，它是基于挑战，它都是经过泛式化处理，是第一手的有效数据吗？所以讲在这方面，一个是叫要素是有效数据的获取，什么是有效数据是你要判别的。第二，通过数据的关联分析对数据进行理解，最后对今后的趋势做一个判断，这是态势感知最初的定义。我们是不是应该从最初来走，我们现在到后面看的很漂亮，图案很好看，我说这个有什么用，看也看不明白。如果看着好看，《王者荣耀》一定做得比它更好看。你对于数据的获取、理解。

基于这样子我有一个要求，如果让我来做态势感知这就是我的要求。第一，目标就是习大大说的全天候、全方位感知网络安全态势。要实时发现网络异常情况，一定是基于行为。对于攻击目标要快速发现，要能够关联分析，快速定位，你才能采取措施。实际上基于这样子，态势感知最后是图形化展示。首先，领导要能看懂、专业人员要看懂，要能处理，非专业人员也能看懂的图，实际上这就是哲学的思维，大道至简，这种图才是态势感知今后要的图。这就是我的理念。

基于这样子，我们画了一个图。我的观点，现在国内没有哪一个公司能够把所有的安全做完，今后一定是一个生态链，人工智能、机器、学习都在用于安全，这是没有问题的。但是我的观点是，今后在很长一段时间里面一定是人和机器的高度协同。就是说，阿尔法GO是19×19，简单问题的复杂分析。安全是什么？安全是复杂问题的复杂分析。全球的人工智能现在大概只有两三岁小孩的水平，你说这个基于安全怎么来做。所以能够做简单的归并那是机器学习能够做的，最后是攻击行为还是误报应该采取什么样的措施，有专业人员做出判断。如果每一块有相关的内容，这个没办法展开说了。如果大家有需要，我们还可以再沟通。

最后，我的理念就是在任何情况下，我都要做到要求是可控制、可管理、可追溯。网络安全，最终需要做的安全是什么？是保证你的数据的安全，数据是你的资产、你的核心，网络是链接。所有的安全或者所有的信息化都离不开云管端，端就是终端，管是链接，你去看最近美国、英国，把网络这块叫链接，所有的3G、4G、5G，互联网是链接，链接有链接的要求。云计算是提供个性化的服务，上面要保证应用的安全、数据的安全，所以核心都是在云、管、端上面。这是需要你主动发现问题、处理问题。你的对手永远不会告诉你他从你这里拿走多少数据，这就是搞安全你应该把自己的系统主动做得更好。在这种情况下，我们的使命就是叫于无声处捍卫国家安全。

我的报告就是这些，谢谢大家。

李洪涛：谢谢邵处的分享。

接下来，有请中国互联网络信息中心胡安磊主任，演讲的主题为“中国域名服务安全状况态势分析——2017”。

胡安磊：非常高兴，今天和大家分享一下一个比较窄的领域或者比较小的领域安全的状况。分三块，第一部分是介绍一下这个事情的背景。大家可能对域名服务不是特别的了解，我简单一下什么是域名服务。实际上我们在每次上网的时候，不管是你访问一个网站，还是在电脑上做其他的事情，基本上都需要一个过程，我需要把一个名字转换成计算机能够识别的IP地址，这样你才能访问到你想访问的服务。域名服务就是这样一个过程，帮助你输入一个名字找到这个服务。

从这个图我们可以看一下，一次域名解析的过程有4个环节在参与。我们通过电脑先找一个服务器，根据你要查的名字去找根服务器，根据你想访问的名字告诉你这个名字，你访问一个DNS的域名，需要去那里的服务器访问，如果是新浪的话就新浪的服务器访问一下，最后新浪自己的全域服务器把IP地址告诉其他服务器，传到终端就可以打开网页，这就是域名解析的大体过程，实际上涉及到4个环节。

我们在做域名管理的同时，在关注整个域名体系的服务安全。从2009年开始就在研究对整个国内域名体系做一个安全方面的监测。在2010年的时候我们正式建设这样的系统，这个系统在2012年、2013年建成投入使用，从2013年开始这个系统不断完善。目前在全国所有省份覆盖3大运营商，部署了几十个监测节点，我们在海外，在东南亚、俄罗斯，我们部署了一些监测的节点。从五个方面有六七十个定测项检测域名服务的专项。我们利用这样的系统，在重大活动的时候我们会做重点的监测或者是预警。

基于我们这个监测平台获取到的数据，我们从2012年开始，每年都会有一个报告出来，就是来分析一下整个年度国内域名服务体系运行的状况、安全状况怎么样，今年已经做到第五期的报告。我下面主要跟大家分享一下2017年报告里面一些比较关键的数据。

刚才提到了域名服务体系有四个环节，最上面的环节就是根服务器。全球有13个，为了保障域名服务的安全，其实13个根域名服务器的管理组织一直在不断地扩充根服务器的数量，尤其是在2002年受到攻击以后，尤其2010年以后根服务器部署速度加快。2017年底的时候，全球根服务器数量达到956个，将近有50%增量的增幅。但是对于我们中国大陆地区来说，在2016年、2017年的时候我们根镜像数量是一样的，在快速扩充的情况有一些脱节。这样的话，其实是不利于根服务器或者是根域名解析服务在国内更稳定、更安全或者是你的解析会更快。

我们对根域名服务的一些重要的情况，做一个简单的分析。根域名服务支持这块，对IPv6、DNSSEC、TCP等网络协议的支持率均为100%，数据包可能会变大，那么就需要支持TCP的协议来支撑解析。在歇息支持方面，根域名服务非常完善，已经达到100%支持。从服务性能方面，我们可以看一下比较柱比较短的，是F、I、J、L根，时间是最短的，相对于其他没有在我们国内有根镜像的根。所以说在国内我们部署更多的根镜像，对于提高域名解析响应速度非常有效。我们同时可以看到M根的解析响应时间不是太长，是因为这个根部署在日本的，我们到日本肯定要比去欧洲、去美国要快。所以说，解析的性能还是跟服务器的部署位置有非常大的关系。我们刚才是把根域名服务情况做了一个简单的介绍。

根域名下面就是顶级域名服务，截止到2017年底的时候全球域名体系中共存1573个顶级域名，较2016年同期新增13个。第一批域名已经完成入根了，但是第二批还没有开启，所以顶级域这块相对比较稳定。顶级域名服务当中解析的情况，从2014-2017年，2014年的时候顶级域名服务使用Bind的软件，比例是90%以上，到2017年的时候已经降到46.7%。NSD在2017年已经达到了38.7%，2016年的时候只有4%。这说明两个问题，第一，Bind的软件是公益性的，近些年受到一些经济方面的困难，所以维护出现了问题，大家尽量少用他。第二，大家还会用这方面的问题，你的软件有这种差异性，能够互相备份，避免一个服务都跑在同一个软件上面。

顶级域名服务在协议支持方面，我们可以看到对各种协议的支持比例在稳步的提升。其中DNSSEC部署比例达到90%以上，因为所有加入根域名服务器里面的必须支持DNSSCEW。IPv6部署比例达到87.4%，这其实是在顶级域方面提供了非常好的基础。

在服务性能方面，不同国家的顶级域，包括商业顶级域是对外提供服务，来保证服务的稳定性和可靠性。平均每个顶级域目前有9个服务地址在对外提供服务，有超过80%的顶级域在对外提供服务。服务地址很多，服务安全性、稳定性有更好的保障。但是同时会带来另外一个问题就是服务器比较多、地址比较多，可能会存在服务数据不一致的问题。我们监测发现有2.2%的顶级域名存在数据不一致的，因为有多个地址和很多服务器提供服务。如果是因为管理上和数据同步的问题，可能我在每次解析的时候到了不同的服务器，可能拿到的结果会是不一样的，可能你访问到的服务也是不一样的，有2.2%的比例存在这样的问题。同时，顶级域名服务做全面域名解析，有3.7%开启了递归服务，这是能够很大地降低你对DDos攻击的防御能力，新加入根区的顶级域存在这样的问题。

再看一下顶级域名服务的解析时延情况。在2017年的时候解析时延相比往年有很大的提升，有超过50%的顶级域名的解析时延集中在100毫秒以内，这说明我们这两年运营商在提速降费上，尤其是提速方面可能做的工作是非常显著的，在域名解析环节也有很好的体现。

再说一下二级及以下权威域名服务。我这个域名注册以后托管在第三方，比如说像阿里云、新网，我会托管在那里解析。还有一种情况，我注册一个域名我自己建一台服务器，自己给自己做服务。这个就是二级及以下的权威域名服务器。通过我们的监测，我们可以分析出来目前国内二级及以下的权威域名服务器有10万台套，这比2016年增加了2万台套，说明我们的互联网发展比较快。它的数量规模来说在域名服务体系里面是最大的，同时跟互联网应用联系最紧密的。终端用户来访问这个网站要解析这个名字，他也是最终的一个目标。所以说二级及以下的权威域名服务器对互联网解析非常重要的。

通过我们的分析看的话，跟顶级域名服务器是一样的，在解析服务器方面是差不多的，但是有一个稳步的下降。在其他软件使用方面与顶级域名服务存在很大的差异，到了二级及以下权威域名服务器排名第二的是微软，说明解析软件的多样性也是在逐步的丰富。

在协议支持程度方面，在DNSSEC和IPv6支持程度方面的进展缓慢，可能需要配合两办提出的部署行动计划来一个大规模的推进。因为只有域名服务器支持了解析，那才能推动，我才能说部署可用了。所以说在这方面的部署方面，二级及以下的权威域名服务器起来有很多工作要做的，而且有34.7%的比例开启了递归服务，安全性会有一定程度的下降。在服务性能方面，二级及以下权威域名服务器82..%已实现冗余配置，平均每个域名拥有7.6个对外服务地址数量，服务性能都还是非常好的。

刚才说的是国内12台套的二级及以下权威域名服务器，同时我们也重点关注了国内300多个重点的权威域名服务器，我们认为三大运营商、重要托管商、重要行业的，比如说金融行业、电力行业等等这些重要的权威域名服务器的安全状况。总体来说，它在协议支持方面，尤其是说IPv6的支持情况稍好于国内的水平，这是IPv6。还有比如说是87.2%，解析时间在100毫秒以内，比国内平均水平略好一点。重点的权威域名服务解析，我们发现二级及以下权威域名服务器还是比较重视服务方面的问题。

第四，递归域名服务。在2017年底的时候，我们国家的递归域名服务大约有11万台套，有1万台套的增加。递归域名服务是最直接面向终端用户，所有解析的请求和结果的返回东西通过递归域名服务器来实现的。在域名解析方面，Bind使用比例快速下降，另外是微软DNS使用比例在明显上升，跟二级及以下权威域名服务器的情况是类似的。在协议支持方面，DNSSEC支持比率只有1.2%。我们新增的递归域名服务器在新增方面存在一些问题。还有就是端口的随机性的程度，端口随机性关系到域名解析的安全性，如果比较差就容易受到中毒的攻击，所以端口随机性越高，受到的攻击成功的可能性就越低。在2017年的时候，端口随机性程度较高的递归域名服务比例已经达到90%，防御能力有待提升。服务性能方面是将近90%的递归域名服务解析时间小于100毫秒。

另外再介绍一下重要的递归域名服务。我们把国内主要有三大运营商，还有一些公开的第三方的递归域名服务，比如说递归云解析，还有114，还有很多第三方的DNSSEC，我们统计了大概有500多台套。三大运营商承担的递归域名解析占比达到国内所有域名解析量的80%，国内所有用户上网行为做域名解析是有80%以上是由三大运营商的递归域名服务器完成的。我们可以看到协议支持方面是要高于国内平均水平，端口随机程度都是比较高的，100%都是随机程度比较高。同时另外一个反向的差距，只有76%的时延是小于100毫秒以内，这是一个相对比较奇怪的现象，我们还需要进一步分析它的原因是什么。

上面是从根域名服务、顶级域名服务、二级及以下权威域名服务、递归域名服务，分别介绍了这四各环节主要的一些情况。

我们从2014年开始研究了一个算法，根据我们从5个方面、60多个监测项监测到的数据对此进行评估。在2017年的时候，权威域名服务总体趋势是向好的。一个很明显的表现就是，安全状况为差的权威域名服务器显著减少，我们看到比例只有10%。同样，递归域名服务安全水平也是在不断提升的，根据我们计算的方法，我们算出来安全状况为优的情况在增加，已经达到70%，相比于2016年有一个非常显著的增加。上面是我主要介绍的情况，就是我们2017年整个域名服务体系各个环节的安全状况。

最后说一下我们的判断和观点。在2017年国家域名服务体系安全状况和以往几年相比，还是有一定程度的改善。但是我们也应该看到，在域名解析不同的环节仍然存在不同程度的安全问题。比如说我们在根域名服务方面，我们最近几年国内的根镜像都没有增加。另外还存在一个问题，我们国家一直没有根域名服务器的管理权，我们希望能够有所突破。在顶级域名方面有1000多个，国内有几十上百个域名是可以注册的，这样的话就对监管部门提出一定的挑战，我们怎么把《中国互联网域名管理办法》落实到不仅仅是国家顶级，只要在中国落地的顶级域名，我们《域名管理办法》的要求很多安全方面法律法规的要求，怎么能够比较完全的落实落地，能够真正的起到效果，我觉得这是在顶级域方面的一个压力。同时，二级及以下权威域名服务器目前来看海量是最大的，它的服务能力也是最参差不齐的，有非常好的域名解析托管商，也有经常出安全事件的域名解析托管商，到底安全水平、运维水平等等怎么样，都是很难把握的。尤其是一些重型和重大型的域名托管商，如果它出现问题的话影响会非常大。在这方面的话，下一步把我们很多安全管理的要求，一些安全监管的范围要进一步扩大，能够监管到这些提供大量权威域名解析托管的服务商。递归域名服务方面，我们首先抓住了牛鼻子。目前来看水平在不断提高，安全状况也是非常好的。同时也有非常多的第三方的递归解析服务，目前来看我们是没有一个有效的手段对它进行监管，这个可能是我们面临的一个比较长期的问题。

这是我今天报告的所有内容，谢谢大家。

李洪涛：谢谢安磊的精彩分享。

下面，有请中国信息通信研究院安全研究所所长魏亮，演讲的主题为“构建共建共治，多方参与的数据安全保障生态体系”。

魏亮：各位，非常高兴今天有这个机会和大家分享一下，我们对于数据安全的理解和研究。现在全球已经进入一个数据驱动的时代，我们数据的总量在爆炸，不断地有很多的数据每天都在产生，有了物联网、车联网以后，每天有巨量的数据在产生。在这个大数据时代，我们看到数据的价值在凸显，通过大数据的分析、通过数据的一些加工，我们可以挣钱。此外，数据的治理也成为一个国家竞争优势新的动力，我们怎么来治理这些数据。我们国家也在关注关于数据跨境流动方面，去年应该有了一些征求意见稿，我们已经看到了。所以跨境数据流动方面我们国家也很快要有一些监管，但是因为现在意见比较多，所以一直在讨论过程中。

除了数据在产生价值的同时，我们看到数据的安全问题也是在凸显，如何有效地应对大数据、人工智能这些新应用出现的同时，数据成为一个迫切解决的关键性问题。facebook的数据被人利用，利用了以后剑桥分析公司用它来影响了美国的大选。从技术上来说，技术本身并不是特别复杂，但是给大家的震惊还是比较大的，给我也比较惊讶。因为我一直觉得，只有说美国利用大数据去影响一些小国或者别的落后，就是在互联网上落后一点的国家。既然美国作为互联网行业的老大都会因为互联网的原因被影响大选的结果，应该来说是非常令人震惊的。第三方应用获取了数据，剑桥通过数据知道了你的定喜好，然后影响了大选。

数据的共享已经成为数据安全中薄弱环节，传统静态安全保护措施失效。你怎么保护它，怎么设边界都没有用，因为分享出去以后别人怎么用你不知道。现在数据共享一般来说，第三方两个公司之间通过合同，但是纸面协议对他的约束能力比较有限。体系抚摸美欧对跨境数据调动进行立法，主权国都希望便捷获取在别的国家一些数据，又不希望别的国家随意访问自己国家的数据。中美有关于司法协作的协议，但是非常复杂，效率很慢。美国一般来说倾向于直接跟公司打交道，要求你拿到一些数据，但是也会有一些阻碍，比如要求微软提供一些数据的时候，微软直接跟他打官司，所以影响很大。

美国最近通过一个（英文）法案，是关于澄清域外合法使用数据的立法，其实就是要能够很容易的获得存储在境外的数据。欧洲做的提案是《电子证据跨境数据访问》，能够提供新的法律工具，就是要合法的做这件事情。CLOUD，如果微软是数据控制者，即使存储在别的国家的数据，他也应该要按照美国的法律来提供。但是他也不是说，至少他表现的不是那么的过分，他还是有一定的抗辩的渠道。在下面两种情况下可以撤销或者修整法律流程，这个就是目标对象不是美国人，且不居住美国。另一个情况，如果数据所在国家是一个符合资格的外国政府，同时有一个立法不允许这些数据出境，这样的话就可以不用向美国政府提供这些数据。符合资格的外国政府是由美国来定的，是比较难的，是有标准的。除了资格之外，CLOUD向外国发出，可以要求美国企业提供美国数据，但是有一些限制条件。也就是说，美国政府可以通过法案向一些外国政府获取数据，外国那些符合资格的外国政府也可以通过这个法案从美国来获取数据。欧盟有一个e-Evidence，欧盟成员国提供什么呢？服务提供者向欧盟居民提供服务。这里面包括两部分，一个是欧盟的数据产生指令，一个是欧盟数据留存指令。这个是国际上希望能够跨境调取数据的一些立法，能够使这些调取数据的行为本身合法，也希望大家遵循这些要求。

基本情况。数据安全实际上是一个比较复杂的，这里画了一个非常简单的生态，这里不应该是政府，而是国家。国家首先是立法，有一个很好的法律体系，其次监管公司、个人、第三方、企业、研究机构，监管他们合法地使用数据。同时还应该建立起信用体系。个人应该来说，对自己的数据有一定的权利，同时他应该有一定的意识，意识到我有这样的权利和保护这样的权利。数据控制者为个人提供服务也提供数据，控制者进行协作进行分析和争执。同时行业协会一方面进行监督，一方面是在行业层面来进行一些行业自律工作。同时，我们不必讳，我们有黑会的产业，这个产业非常大，里面有一些黑客会获取数据，把非法获取的数据进行出售、诈骗等等这些工作。这里包含了很多，所以说数据安全的工作不是简单的哪个部门发一个指令或者出台一个《办法》就能解决的，应该是多个生态圈里面所有的都要做出自己的努力，才能做好数据安全的工作。

我们看看这些要素，现在看到有几个方面要素，立法、监管、诚信体系、技术、公众意识、行业组织。诚信体系是政府或者民间层面进行自发手段。行业组织在民间层面可以产生一些业界的需求，有一些业界的共识，达成一些业界的标准，然后形成行业的自律。公众意识属于民众基础，一方面要提升自己的意识，一方面可以反作用于政府的立法或者执法，很多立法可能出于一个事件的触动，公众关注了就有这些立法。还有技术属于支撑的手段，为企业提供一些保障。

看一下立法，2012年有一个人大关于加强网络信息保护的决定，2016年有一个电信和互联网个人信息保护决定，2017年的《网络安全法》，这个可以作为依据，我们有行政法规和部门规章。我们国家现在可以看到比较分散，数据和个人信息保护分散在各个法律和部门规章里面。同时，刑法立法先于民事行政立法，而且入刑门槛很低，50条就可以入刑，有一定的震慑和威慑能力。同时，量刑标准也有一定的创新，不同的数量和敏感程度来区分量刑。我们现在有一个初步的法律体系，但是应该来说对数据安全没有一个统一的立法。目前法律界定里面责任主体是电信运营者的一些责权都没有明确。监管现状涉及的部门比较多，包括工信部、商务部、公安部等等，执法的是公安和国家安全机构，但是模式还不是特别清楚，机制也不完善，现在还是实践驱动，在融合领域各方面划分并不是特别清楚。

存在的问题就是没有一个统一的执法机构，缺乏常态化监管机制、缺乏融合领域监管机制，同时处罚偏轻，行政处罚最高罚款3万人民币，这个对互联网企业来说简直就是九牛一毛都算不上。从诚信体系来看，已经有了一个名单。互联网企业也是在做一些诚信体系，最典型的就是给个人做诚信体系，也正在进行中。现在诚信体系中应该把数据安全和个人征信数据安全，需要进一步明确需求。从行业组织来看，互联网协会有一个个人信息保护委员会，12321可以进行受理举报，可以受理不良与垃圾信息进行举报。还有行业标准化。现在行业组织比较少，力量比较薄弱，同时现在都是一些全国性组织，地方组织比较少。从意识上来看，总体上企业和个人的数据防护意识偏低，但是不断提高中。近年来反诈工作做得轰轰烈烈，大家对个人信息保护的意识有了明显的提升。意识是在增强，我们可以看到了。

技术应该来说数据安全防护技术很多，比如说身份认证、访问控制、安全审计、异常行为监测预警、数据加密等等很多。这些技术是在不同的环节中应用，比如说产生环节、存储环节、使用环节、共享环节、销毁环节，这些环节中都是要利用到不同安全相关的技术。

产品上来说，安全产品不少，正在积极研发各种产品，数据库的安全审计、漏洞扫描、模糊化处理等等，这些都在做。现在数据安全技术也是在面临一些新的挑战，比如说在大数据环境下，原来很多技术适用性不能满足新技术、新业务，不能满足海量的数据。还有匿名化技术，有一些还没有完全使用起来，还在过程中。

最后就是一些对策建议了，需要“共建共治，多方参与”才能做好这方面的工作。首先从国家层面上要制定完善数据安全和个人信息保护政策法规，现在有很多法规，但是不全面。我听到有一些数据安全的《办法》正在制定，我们希望看到泄露了以后对被泄露的被害人有一定的赔偿，这样对他的威慑力大了很多。你偷了50条敏感信息可能会入刑，没有把数据保护好的企业到底有多大责任呢？泄露用户密码的企业写了一个道歉信，这件事就过去了，企业应该承担更大的责任，不应该就罚几万块钱就算了，不能很好地保护用户个人信息的话，就不应该收集它，而且丢失了就要重罚。然后要完善监管制度，加大处罚力度，监管的机制不应该是事先驱动，不应该是出了事罚他，而是有事前、事后的监管。然后要建立政府层面和行业层面的诚信体系，有了诚信体系以后出了一次事情以后，他可能做别的生意或者其他的运营都会有影响，这样对他有更大的威慑力。同时要加强行业自律，不可能所有都是从政府层面通过处罚来解决，很重要的就是行业层面要有行业自律和行业共识。提升公众意识，丰富用户个人信息保护手段。你有了足够的意识，那些企业不敢随便的过度收集信息或者是滥用信息，或者是不加保护的把这些数据分享出去。同时从国家层面还要加强安全技术研发和产品化，有了足够的技术做保障，在这些新技术、新业务不断层出不穷，技术融合。大数据时代、人工智能时代才能够通过技术来保障我们用户信息的用户数据的安全。

今天分享的就是这些，谢谢大家。

李洪涛：谢谢魏所长的分享。

下面，有请绿盟科技副总裁宫智，演讲的主题为“互联时代的融合安全”。

宫智：首先很感谢主办方，还有CNNIC邀请我来做分享。作为一个压轴的，时间上我会尽量往前赶赶，也感谢大家耐心等待。我这块的内容是从一个安全产品或者服务以及解决方案的提供者角度，来说一下安全目前的情况，以及分享一下我们的一些想法和实践。

其实前面很多专家都说了，在当前数据化转型是一个目前非常火的一个话题，各行各业。这个变化其实对于安全来说就是带来了很多的机遇，毋庸置疑，安全这两年为什么这么火爆，就是因为互联网的发展，互联网快速的发展带来很多安全问题，安全好像似乎是网络自身所带的缺陷一样。所以对于我们安全公司来说，也带来很多机遇。

这是IDC的报告，这个报告只能说明增长的情况。实际上我们中国在安全这块的投入比例相对于美国来说，还是比较低的。美国大概占4.8%，而中国在IT里面的占比只有1.8%。前面的领导也讲到了，国内目前对安全这块的投入还是不够的，无论是政府也好，还是企业也好。

下面再分享一下我们公司在今年4月份刚发布的《2017年网络安全观察》，其实前面的领导从更大的范围也做了一个详细的解读，我这里面只说几个好玩的。软件是一个非常热门的关键词，基于对受害人来说是两难的境地，我到底该不该给他钱，我如果不给钱我可能会损失我的重要信息，你可以想办法破解，但是都是有成本的，所以这是一个成本的问题。我宁愿付出一万块钱把数据要出来，还是我花两万块钱做防范。这对我们安全服务的提供商来说，我们如何为这些中小客户提供更便利、投入产出更高的安全方案，这是对我们的一个思考。另外一个就是攻击，能看到更多的攻击还是来自于已知的漏洞、已知利用问题来攻击，大家对安全意识上还是不足。很多的企业，可能他们都没有这样的意识。

既然是研究做安全的，肯定要研究一下攻方的变化，我做了一个简单的总结。互联网发展之后对于攻击者来说，他们的发展也是非常快，他们也采用了很多的技术，自动化、智能化、系统化，现在的攻击不是单一攻击，而是组合拳，会用多种方法来做这个事情。另外一个更加可怕的是商业化，包括美国那边有政府研究的武器库，暗网里面有很多攻击武器、攻击工具公开售卖，这是一个高度保密的。还有一个就是组织化，黑客组织不说。现在上升到有政治层面或者是政府层面。

这个就是前面也说了，实际上对于攻击也好、互联网的变化也好，对于现在的挑战还是一个对抗。但是这个对抗不是平等对抗，一个在明，一个在暗。只要找到一点漏洞，他就可以成功，而你需要做全方位的防护，这始终是不对等的。在不对等的条件下你要做好这件事情，或者你有什么办法做好这件事情，这就是一个挑战。这里用一个业界这两年比较流行的攻击链的方式，大家可以看到，我实现一个攻击经过这样一些步骤，而对于你的防护者来说，你在任何一个阶段看到的一个问题，也许它的风险等级不高，你没有重视。但是当这些问题在不同阶段串起来的时候，它可能就实现了一次攻击，而你会忽略掉或者错过它。这是对于我们防护来说或者对于一个企业来说，你去防范安全的时候里面的挑战，你不能在一点去防范，你可能需要从头到尾全生命周期去防范才能达到你的目的。

这是对于我们作为安全产品也好，或者作为安全服务业好，我们的一个感觉。在过去，我们在为大家提供安全产品、安全服务的时候，我们的产品可能是基于规则的防护。最典型的就是签名，病毒有病毒的特征，有病毒签名的代码是有特征的，包括数据报文是有固定的二级代码，这是过往最简单的防护方法。再就是静态的，也就是说它是对已知问题来防护或者用已知防已知，可能有小的变化，但是无论如何是用已知防已知。还有被动的，我给你挡在门外，它来了之后我把你及时的截获掉，但是这种是被动防御性。再一个就是局部的，以前我们叫网络安全公司，这已经有一个局限性了。是不是你只做网络安全的，你只关注网络安全，而现在实际上大家面临的问题或者一个企业面临的问题，可能不只只是网络层面的问题，可能是应用层面的问题。解决这个问题来说，不单单涉及到数据层面、网络层面、应用层面，甚至是业务逻辑层面也好，多层次的问题。这种变化对于我们到现在为止产生的调整是什么样的？需要我们的安全能力变成动态的，需要能够去适应攻击者的变化，而你采用相应的变化。再就是主动的，不是被动等它来了，你要主动做一些事情、做一些预防或者是叫风险控制。

拿一个这两天发生的一个事件说一下，滴滴这两天刚好发生了一件很悲惨的事情，有一个叫顺风车的不幸被害的，司机已经找到，实际上他已经跳河溺亡了。滴滴我还是非常尊敬的企业，它自己做了一套很好的安全防范体系，但是依然会发生这样的事情。这样的事情你会想有没有办法去防止它、预防它，不是说等到那个人拿出刀了，你说我跟他打，这样实际上就是危机都已经到眼前了你再去做事情，已经是晚了。我们要做的是预防犯罪，也就是说，实际上当这个空姐她在叫顺风车的时候，我在派单的时候不要派这样的人接单，不让这两个人产生交集就可以防止这样的事情发生。这是我们做安全的时候理念，我们在开始的时候就不要等到人家走到你的门口了，而你去做事情，而是要走在前面。现在整个从防护来说变成一个系统性防护。这个是对于防护者或者说对于做安全，希望能够为大家提供安全方案和服务来说的一个要求，就需要这五方面的能力。还有就是智能化，实际上AI这两年非常火，在安全领域来说，智能是对安全产生非常大的冲击或者带来非常大的变化。

我今天主题说融合安全，当时也在想为什么叫融合，用整合物的集成好，还是用融合好，其实融合更合适。第一方面是技术融合，安全到现在随着互联网的发展来说，它需要采用更快的能够采纳新的技术，包括人工智能、机器学习等等。这些技术的采用才能够让我们的安全，为我们的安全提供者、为我们的安全防护能够实现你的目标。在大数据技术出现之前，大家都知道要去做一些关联防护、关联分析。我把防火墙IPS相关的东西日志产生出来，我能做一些关联分析，大家都想过，但是很难找到一些相应的技术支撑，你就没法实现，你就做不成。当你技术出来之后有为你提供这样的便利了，你就应该快速采用这样的技术。第一点就是需要做技术融合。

再就是产品融合。我们不能够期望用一个产品解决所有的问题。现在目前所有的安全问题都是需要多个产品组合来解决问题。

再一个就是数据融合。现在信息不能是孤岛，特别是对安全来说一定要做事件的关联。还是拿滴滴来说，都知道滴滴是给乘客和司机画像的，要知道有什么特点。这个画像来说，对任何一方来说都是孤立的，但是关键来说是怎么做关联和匹配。网上也在说，我们平时在点评司机，实际上司机也在点评乘客，一样的。如果你发现这个乘客的标签比如很漂亮，当作为很漂亮的标签在半夜12点打车的时候，漂亮本身认为是一个低危的，但是一个时间是半夜12点，单纯半夜12点也是一个低危事件，两个低危事件在一起可能危险程度就变高了。很多时候你对于一个威胁的判断就是对于多种数据综合的决策。

再一个就是能力的融合。前面有一位领导也分享过，过去我们安全厂家来说卖的是盒子，我卖了一个防火墙我就不管了，用不用的好可能是用户的事情。但现在来说，对我们来说应该发生变化了。我们交付给用户应该是安全的能力或者使他业务安全的能力，这种能力的达成就是需要你的设备自身的能力，以及用好这个设备的能力，我们叫运营或者运维的能力，这种能力的组合才能够真正的为用户实现安全的赋能。

再一个就是业务的融合。我个人认为这个是目前或者是对于安全从业人员来说是非常困难的事情。如果你真真正正要达到安全的结果来说，其实在业务层面你就需要去深入这个客户的业务过程，你才能够真正为他起到一个守护的作用。

这个是我今天说的融合安全是一个什么样的，实际上是由这五方面来组成的。

web科技我们有自己的实践。我们在利用机器学习在外部攻防方面，不只在这个方面让它发挥更好的作用，实际上让我们防护脱离了过去单纯的依靠规则的防护方式。而是利用机器学习的方式基于行为模式来去判断，这种误报率和准确率都有大幅的提升。再一个就是云计算，这是这两天非常火的，包括整个企业在往云这方面来做，不管是公有云也好，还是私有云也好。这是我们构建的一个基于云计算打造的一套云安全的方案，这里面整合了非常多方面。不同的安全模块得到充分的组合，它形成一个安全能力池，这个是最核心的概念。基于这样的安全能力之上，我们进一步做了业务的编排，最后交付给客户的是安全能力。

再一个就是数据安全能力。刚才说了，再数据的融合我们通过各种渠道，包括我们的产品、包括第三方合作伙伴，包括一些爬虫，包括我们通过安全服务也好，我们可能会获得各式各样的安全数据。对于这些数据我们要进行加工过滤，规则化，最后会形成安全的知识库、信息库，最后变成情报。这些情报不是单纯以情报的形式存在，我们会把情报转而运用到安全产品、安全平台上，让情报发挥作用，让情报来驱动整个安全的运营。这个是说数据融合后带来的好处。

再一个就是安全能力的融合。现在的防护或者说现在安全的焦点不能是孤立的网络节点，而我要围绕的是客户资产或者是客户业务。实现这样安全的时候，你就是要多方能力的协调，事前的监测、事中防护、事后响应取证等等，这样的闭环才能够达到真正实现了安全的强能力，通过这种运营使安全的响应能够达到更及时和迅捷。

刚才说了，安全我们需要跟业务融合。其实实际上大家在做一些业务开发的更能理解这个，这个业务从代码开始，实际上就开始需要有安全来介入了，安全要做代码审计，其实这就是比较低层次的。在高层次的要做业务逻辑审计，看看业务逻辑有没有漏洞。还有业务过程或者是操作过程，整个这个业务链条来说，你可以发现每一环节都需要安全的加入之后，你最终业务上线之后才能够实现相对安全，其实没有绝对安全，安全都是相对的。这个过程不容易，因为这个过程是需要数据双方充分的信任，特别是你的数据让第三方来做的。在一个公司内，安全部门和业务部门经常会打起来的，因为大家出发点不一样，业务部门会觉得安全拖我后腿。所以这件事情很重要，但是真正做起来的时候其实是很不容易的。

今天只是简单分享一下，我们认为目前来说对于安全，我们认为是需要有融合是最核心的，包括从技术、产品、数据等等，包括能力。最终我们绿盟在2015年就提出了一个框架或者是一个体系，就是智慧安全的框架。这个框架也是按照我们融合的理念来做的，最核心的就是说，实际上我们需要在客户侧把整个安全能力，包括绿盟的能力，包括第三方的能力整合起来，跟绿盟云端能够做整合。再就是我们充分利用了本地运营能力，以及设备智能化的能力，人和设备的一个结合。这样一个综合立体防护是希望最终能够为客户打造一个完美的安全方案。

最后，因为前段时间刚好看到一段新闻，这是今年2018年普利兹克建筑奖获得者说的“当生活方式和建筑融为一体时，生活便变成一场庆典”。从方便人们生活的角度去设计的，对做产品安全一样，我们做的安全比较和客户的生活充分融合以后，才能够为客户提供更好的产品效果。

谢谢大家。

李洪涛：谢谢宫总的分享。在此，再次感谢今天下午各位报告人做的演讲，同时感谢各位参会的嘉宾、媒体朋友。

本场论坛到此结束，谢谢大家。