抓住机遇打造好
中国第五空间的安全基石

中国计算机学会计算机安全专业委员会　主任
公安部第一研究所 原所长研究员
严　明

据有关机构发布的报告，截止2015年6月，我国网络个人用户规模达到6.68亿，其中使用手机上网的用户达到88.9%。

中国域名总数已为2231万个，其中使用“.CN”的域名总数为1225万个，占中国域名总数比例为54.9%，使用“.中国”域名总数为26万个。

中国网站总数为357万个，其中.CN下网站数为163万个。

有人说，中国已是名副其实的“网络大国”。

至今，数字化和网络化已经深入到我国的各行各业：电力、交通、通信、医疗、金融、教育、社保、工业农业乃至国防和民众的日常生活等，都已经离不开信息网络和信息。国家、企业、民众的方方面面都已经离不开网络与信息的支持。

我们曾经把网络叫虚拟世界，现在看来网络已经是真实世界的越来越重要、越来越不可缺少的部分。无论你上网还是不上网，你都早已离不开信息网络。

美国毫不含糊的把网络空间（Cyberspace）确定为其继陆、海、空、天的第五个国家安全领域。公开宣布，谁攻击了美国的网络，美国将动用一切手段包括战争来反击。

我国信息化的建设和深入发展始终伴随着来自不同方面的安全威胁，我们必须对此有充分认识：

Internet或者因特网是美国构筑和控制的一个信息网络，这个网络的核心设施域名服务器大部分都在美国本土。我国是签约接入国，所以，本质上中国因特网是美国因特网的一个分支，我们其实是因特网的用户大国；

美国政府曾经宣布计划将ICANN互联网域名管理权移交，但是又说不会移交给联合国。他说希望2015年移交给“全球利益攸关体”，但前提是有满意的解决方案。

有专家说，中国的信息安全在以思科为代表的美国“八大金刚”面前形同虚设。在绝大多数核心领域，IBM、思科、微软、高通、英特尔、苹果、甲骨文和谷歌这8家企业都占据了庞大的市场份额。

电信及互联网，政府部门，军工企业，中国高校，金融行业，海关、公安、武警、工商、教育，铁路系统，民航，机场、码头和港口，在石油、制造、轻工和烟草等行业，电视台及传媒行业，……都占据了超过一半的份额。

- 在软件系统方面，微软、谷歌和苹果，甲骨文等公司前些年在中国几乎做到了全覆盖。中国包括政府部门、军队、武警、军工企业等在内的所有单位，几乎100%使用美国的操作系统和办公软件。一些储存重要信息的数据库软件以及工业控制系统，也均为西方高科技公司所研发的。

一线的芯片（Intel80%），主流操作系统（MS 96.23%）和数据库，各种应用软件等技术和产品也基本为国外厂商所垄断；

来自国家互联网应急中心(CNCERT)的最新数据显示，中国遭受境外网络攻击的情况日趋严重。无论是按照攻击服务器数量还是按照控制的中国主机数量来排名，美国都名列第一。

美国早已制定了完整的网络空间战略，认为网络空间(Cyberspace)是远在领土、领海、领空和太空之上的第五个重要空间。

美国成立网络司令部后，提出全面发展先发制人的网络攻击能力并将中国列为主要网络战对手。频繁进行网络攻防演习。已经进行了网络风暴I、网络风暴II，其网络风暴III的规模和参加国达到空前水平。去年，美国防长声称其网军已经达到6000人规模。

位于佛吉尼亚州阿灵顿的美国网络司令部在为网络风暴3演习做准备

其实棱镜计划只是美国众多网络战计划中的一个。新加坡联合早报刊载“量子计划的潘多拉梦魇”直指量子计划作为美国国家安全局的全球监听计划。其能够在对手的电脑没有连接互联网的条件下保持监控能力、盗取其资料和对其发送恶意软件进行网络攻击。据称这项技术早在2008年就已经开始使用。

NSA（美国国家安全局）还有一个“涡轮”项目，其为一个名为“拥有网络”(Owning the Net)的大型项目的一部分。利用它，NSA部署并运行着“Turbine”恶意软件植入系统，以及代号为“Turmoil”的数据监控传感器网络，用以监控全球整个互联网上传送的数据包。

其Turmoil”的 “分拣器(selector)”自动识别被监控目标的数据。NSA能根据用户是否使用谷歌、雅虎、Skype、飞信和QQ可能还有微信等信息来锁定监控目标。 其使用的一种叫分拣器的工具可以对全球的计算机标识符、注册的设备、加密密钥、网络信息、用户的线索进行收集分析处理和攻击。

NSA拥有多种恶意软件工具。如，“CAPTIVATED AUDIENCE”（迷惑听众）控制目标计算机麦克风，记录对话。“GUM FISH”（粘鱼）控制目标计算机摄像头拍摄照片。“FOGGY BOTTOM”（模糊的真相）能记录互联网浏览历史数据，并收集用户登录网站和电子邮件帐户的用户名和密码，“GROK”（感知）用于记录键盘输入，而“SALVAGE RABBIT”能获取连接至计算机的U盘中的数据。同时还拦截通过VPN传输的数据和VoIP数据。

- 方滨兴院士在他的一篇文章中介绍了美国诸多的网络战武器：
- 专门攻击USB的**水腹蛇**和**水腹蛇2**；攻击键盘的**恶卵**；攻击视频线的**疯狂主人**；攻击硬盘的**发怒僧侣**；攻击BIOS的**交换**；攻击总线的**后勤诱捕**；攻击苹果手机的**出轨吉普**；攻击WINDOWS的**图腾幽灵**；攻击GSM手机SIM卡的**松鼠集**；攻击GSM基站路由器的**飓风Hx9**；攻击WIFI路由器的**床头柜**；

- （续）
- 攻击网络插座的**火步**；攻击思科防火墙的**喷气犁**；攻击华为防火墙的**拇指水**；攻击詹博防火墙的**给料槽**；攻击华为路由器的**源头**；攻击詹博路由器的**蒙大拿学校**；攻击服务器的**神级跳跃**……。
- 相信这不会是其武器库的全部。

安全专家在硬盘固件中发现了网络间谍程序，这些程序非常难以被检测或者删除。来自卡巴斯基的研究者公布了该恶意程序用来“Phone Home”的URL地址，NSA利用这些随机、凌乱的地址来收集硬盘上的敏感数据。

下载完整报告："Equation group: questions and answers" PDF

对于斯诺登公布的一份文件指称美国国安局和英国政府通信总部侵入荷兰手机SIM卡制造商金雅拓公司并窃取加密密钥，秘密监控全球数十亿用户的电话、短信和电子邮件。美国海军上将迈克尔·罗杰斯（Michael Rogers）在华盛顿的一个论坛上对此做出回应称：“显然，我不会道明具体细节。但我需要指出的一点是，我们完全遵守了法律。”他说，美国的情报以及执法机构需要通过合法手段，来打破并进入到那些越来越缜密的操作系统内，比如由苹果和谷歌开发的操作系统

路透社去年报道，新西兰政府通信安全局(GCSB)对全球进行了监控，并把搜集到的情报传递给美国NSA以及澳大利亚、英国和加拿大的情报机构。这4个国家和新西兰一起组成“5只眼”情报集团。

调查性新闻报道撰稿人尼基·黑格对电视一台记者说：“如果只是为了新西兰自身，很难认为我们会针对那些国家开展高技术间谍活动。”“唯一合理的解释是，我们这么做是在尽责任，或者说在为与美国结盟付费。”

美国中央情报局(CIA)局长约翰·布伦南曾宣布，将对该部门进行大规模重组，并将着力加强网络情报搜集的能力。

根据重组方案，中情局将中情局将现有人员和资源分配到10个新成立的行动中心。这10个中心可按地域和职能划分为两类，包括反恐中心、防武器扩散中心、中东中心以及东亚中心等。每个中心由一名助理局长直接领导。

最近，奥巴马在马里兰州的一个美军基地说：“我们可以选择在这一领域展开竞争——我保证，只要我们想赢，就一定能赢——还有另一种选择，我们可以达成某种共识，确认网络战无意欲任何一方，然后建立某些基本的行为准则。”

“我们向中方明确表示，无法接受他们进行的某些行动。”奥巴马说。

面对美国的网络霸权，欧盟宣布将建立自己的网络系统，巴西提出要重新铺设自己直接通往欧洲海底光缆。

而美国学者高登M.哥德斯坦 撰文“因特网山穷水尽？”分析网络霸权带来的重重危机。

但是斗争仍然是实实在在的进行着。

BBC的报道也指出：“中方称自己才是美国网络攻击的受害者，而**斯诺登曝光的美国情报印证了北京方面的说法。**”

《纽约时报》19日报道称，中国和美国正在就签订两国首个网络空间方面的军备控制协议进行谈判。有关官员透露称，美中两国或将通过协议相互承诺彼此将不会在和平时期率先使用网络武器攻击对方的关键性基础设施，攻击目标包括发电站、银行系统、手机网络、医院等。

- 据报道，中美双方在习主席访美期间一直都在紧张的谈判中，希望能在中国国家主席习近平到华盛顿进行国事访问时达成一项协议。
- 25日，国家主席习近平访美的成果清单公布，其中互联网领域的成果涉及6项之多。
- 沈逸表示，他印象最为深刻的是“中美双方同意，建立两国打击网络犯罪及相关事项高级别联合对话机制”这一条，因为“很新，而且以前很少谈得如此细致”。

我们当然支持签订这种类似于控制化武、生物武器和核武的协议，它反映了网络战对人类的巨大危害。一旦发生恐怕没有胜者。

但是确保其有效执行有赖于相关方防卫和对抗实力的平衡。

我们的信息安全产业就是要在如此巨大的威胁和压力下发展。

- 新技术的应用也不断地带来挑战。诸如云计算、物联网、移动网络、大数据、智能化和三网合一等等信息应用，也不断的暴露出安全问题，不断地提出安全的需求。
- 最近的一个例子是：

- 2015年9月18日中午，乌云漏洞平台披露了非官方Apple iOS Xcode开发工具会向iOS应用中植入恶意代码（XcodeGhost） 。苹果设备上的 APP 都是由苹果 Xcode 开发工具所编译，但由于Xcode，在苹果官方商店安装下载会非常缓慢，很多开发者会在网盘或迅雷下载，这直接导致了本次感染事件的大规模发生。

被植入恶意代码的 iOS 应用会向 C&C 服务器上传信息，具体信息包括：时间、应用名字、应用标识ID、设备名字与类型、系统区域及语言、设备唯一标识UUID、网络类型。通过对APP Store上已发布应用的分析，大量知名应用遭受感染，其中包括微信，滴滴打车，高德地图等知名应用。

截止到2015-9-19，在互联网上仍然可以找到大量的非官方Xcode下载：

- 人们已经开始对苹果的低调和慢反应表示不满。终于在9月21日，苹果公司表示正在对iOS App Store 进行清理，删除其中的iPhone和iPad恶意应用。
- 这是苹果公司首次承认发现批量恶意软件成功绕开苹果的应用审批流程进入到他的软件商店中。

- 9月24日，据外媒报道，苹果推出了更新版操作系统iOS 9.0.1。苹果公司声称，这一更新系统将能够修复系统的一些漏洞。

- 国外安全专家莱恩.奥尔森表示，“这是一次重大事件，其他黑客也有可能效仿本次攻击，…这种攻击很难抵御。”
- 奇虎360早在本月22日就在其官方博客中公布，已经发现有334款应用受到了XcodeGhost 的影响，而苹果至今拒绝透露其发现有多少款应用受到影响。

- 但是事情可能还不止于此，本月22日有消息说，“已经确认Unity-4.x的感染样本恶意代码和XcodeGhoxt的逻辑一致。”而且感染面还在扩大。
- 有专家提出怀疑，称其“看来是一个系统筹划，长期耕耘”的威胁。

我们讨论我国的信息安全产业发展，如果脱离了这些背景，只局限在个人隐私和企业团体的商业机密、财产利益上。就会忘记了对于整个民族的生命线和国家国土安全的更大的威胁。

- 2015年7月22日晚美国财富杂志发布2015年世界500强企业名单，中国上榜企业继续保持强劲增长态势，达到106家，比上年度增加6家，上榜企业数量稳居世界第二。美国上榜企业128家，数量与上年度持平。
- 本年度世界500强的入围门槛提高至237.2亿美元

- 这当中和信息化有关的中国企业有：
- 中国移动（55）、中国电信（160）、联通（227）、华为（228）、联想（231）、电子信息产业集团（366）、广达电脑（389）、大唐集团（392）、仁宝电脑（423）等九家。其余大部分是能源、金融、贸易、粮食等产业领域。（福布斯的排名有所不同，而阿里巴巴在内）
- 而美国的128家中高技术企业特别是信息行业的企业所占比例极高。

- 同期，美国网络安全风险投资公司评定的“最热门，最具创新”的网络安全企业500强，我国只有四家入围，他们是：**安天实验室**（95）、**山石网科**（142）、**杭州安恒**（314）以及提供指纹安全技术的**印象认知**（412）。美国占了八成，包揽了前九名。

- 我国的信息安全产业市场无论是和自己的信息化发展比还是和国际同业比差距都非常大。
- 例如，我国超过十亿规模的网络安全厂家加上相关行业的厂家，如加解密和特殊业务需求的据最新统计也就十多家，等其总体规模、实力和需求差距非常大。

- 根据赛迪发布的2014-2015信息安全产品市场年度报告称，我国信息安全市场在2014年达到了226.8亿元人民币，增速为18.5%。
- 有评论说，一个赛门铁克公司的规模就和我国全部信息安全产业加起来差不多。

- 美国强大的IT产业包括信息安全产业不仅构成了美国强大的经济技术实力，也成为其称霸世界信息化和信息网络的坚实基础。
- 我们中华民族的强国梦，没有强大的产业其中包括信息化和信息安全产业作为基石也是不可能实现的。
- 产业的规模取决于市场的规模。

市场规模取决于投入规模，我国在信息化建设中在信息安全方面投入比例和其他国家相比是什么情况呢：

美国的信息系统建设用于安全的投入大约在25-30%

欧盟的信息系统建设用于安全的投入大约占总投资的15-20%

据我国有关部门统计，我国的信息系统建设中用于安全的投入大约只有3-5%（1%）

- 不改变这种状况，讨论我国信息安全产业的发展就是空谈。
- 目前，有利于产业发展的情况在逐步展现：

- 对我国网络与信息安全产业发展具有决定性影响的大事是，国家网络安全和信息化领导小组的成立。

中央网络安全和信息化领导小组由习近平亲自任组长；李克强、刘云山任副组长。

中央网络安全和信息化建设领导小组的规格高、力度大、立意远，他统筹指导中国迈向网络强国的发展战略，在中央层面设立了一个强有力、具有空前有权威性的网络安全领导机构。是我国信息网络安全的划时代的事情。

这是中共落实十八届三中全会精神的重大举措，是中国网络安全和信息化国家战略迈出的重要一步，标志着这个拥有6.68亿网络个人用户的网络用户大国加速向网络强国挺进。

- 中央网络安全和信息化建设领导小组办公室的成立使得各项工作得以落到实处，有望结束我国一段时间以来的“九龙治水”状态。

- 对于我国信息安全产业的发展，有关专家一直在大声呼吁。我国知名的信息领域院士倪光南提出“新形势下需重新定义信息安全产业”，崔光耀提出“信息安全产业战车驶入机遇期”，沈昌祥、何德全、方滨兴等院士也都中各个方面发出呼吁和建议。

“两会”上，政协和人大代表们再次以空前的关注度聚焦网络与信息安全，国产化成为提案的重点，信息安全立法、加强电子商务管理、保护个人信息安全信息安全、加强基础设施保护等都是讨论的热点问题。

- 好消息是，国家正在落实网络与信息安全的责任管理制度，改变在信息化建设中信息安全建设的投入不足的现象，形成和我国信息化建设和信息安全需求相称的信息安全市场规模。

总的来看，有利于产业发展的因素越来越多：网络强国目标的明确后国家支持的力度在加大；相应的信息安全审查制度和政府采购的导向性会给国内安全企业更多的机会；法制的完善和责任的明确以及政府采购政策的导向会有利于形成健康的产业生态环境；随着国家、政府、企业、个人对信息安全的重视程度的提高，投入越来越大；

- （续）
- 一个有趣的现象是最近股市的大起大落中，信息安全产业似乎一枝独秀，体现出投资者对于中国信息安全产业的信心和投资热情持续高涨。

- 一位公安系统从事信息化建设的人士说：“前几年，我们主要采购IBM的产品。但2014年之后，所有的订单均签给了华为、中兴、浪潮、联想，八大金刚的东西，都要逐步换下来。”
- 但是，性能上的差距使得更多的用户在选择上有点两难
- 国外厂商的积极应对也使得竞争更加激烈

- 我国提出的“一带一路”和“互联网+”也同时给了我国信息安全产业发展的新天地，将竞争提升到一个新的层次，在这方面华为、中兴、联想阿里巴巴和腾信做出了榜样
- 国势给了我们机遇
- 关键是我们必须抓住机遇，发挥自己的特点形成自己的优势，真正强大起来

- 方方面面的事实，都在向我国的信息网络安全产业发出呼唤，或者说都在向我们的信息网络安全企业展现出极大的需求和发展的可能。

- 建成网络安全强国的要素很多。和其他安全领域一样，我们需要有**结构完整，行动协调，技术先进，实力强大**的产业作为构建网络安全强国的基石。

- 国家应该实施“**统筹规划、协同创新、公平竞争**”的政策，构建健康的产业生态环境，来实现建设我国“**构成完整，行动协调，技术先进，实力强大**”的网络安全产业

- 我国信息安全市场在不断发展
- 赛迪发布的2015-2017年中国信息安全产品市场发展预测是：
- 2016年市场规模将超过370亿人民币
- 2017年将达到462亿人民币以上
- 这也许还是估计不足的。

- 差距就是机遇
- 需求就是市场
- 创新才能成功
- 团结就是力量

结语：

习总书记在十八大谈到了实现中华民族伟大复兴的中国梦。他说：“没有网络安全就没有国家安全，没有信息化就没有现代化”。实现中国梦必须实现我国高度信息化的梦想，确保我国网络与信息系统安全是实现中国梦的必要条件，让我们共同努力，在中华民族复兴的伟大事业中做出应有的贡献。

谢谢！