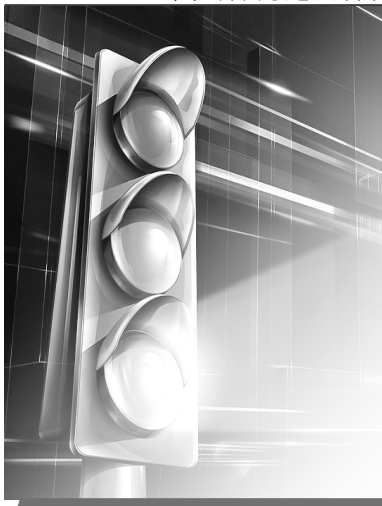

[前　言] 在本刊连续 9 期刊登资深安全专家谈“网络战”的专题之后，本期国内知名安全厂商启明星辰也参与到“网络战”这个话题中来。在这一期，启明星辰的安全专家翟胜军分析了国内外“网络战”的异同，并将网络战从国家间的政治对抗延伸到人们生活中的安全攻击与防御中来。他提出了一个新颖的观点。他认为网络世界最大的特点不是连通，而是开放，有了它海纳百川的“胸怀”，人们才可以迅速融入世界的每个角落。但没有限制的开放就意味着不安全，只有在网络中建立了良好的防护措施，保持网络的“清洁”，才能把网络威胁消弭于无形。在他看来，不能说网络是不安全的，应该说没有管理的网络是不安全的。要在网络战中赢得胜利，就必须建立像交通中“红绿灯”一样的管理措施。

网络战也需要“红绿灯”

本刊记者　周　雪

本世纪初，美国战争防御体系从“四维”空间开始扩展到信息通信领域，在 2009 年美国成立网络司令部之后，“网络战”俨然已经变身为未来战争新模式。启明星辰安全专家翟胜军认为，网络战是网络发展之路上不可避免的一个形态。他解释道，随着互联网的兴起，国家之间的“界限”开始模糊，每个国家的“内部”网络都连接到互联网上（很多网络自称使用单向通信技术连接）。且不论是利用互联网也好，还是被互联网利用也好，互联网都已经成为连接各个国家信息互通的公共通道。利用互联网进行国家之间的入侵、攻击成为可能，互联网的控制权也就成了战争争夺的新“战场”。

保护好网络是国家军事实力的体现

虽然被称作是战场，但信息时代，战争的形式也在不断变化：从地面到海上，从太空到信息，战争方式进入立体化、空间化、数字化，成为多纬度的战争形式，国家入侵也从领土占领发展到精神侵占与信息阻断。网络安全已经成为国家安全的一部分，它不仅控制着有关民生的基础设施，而且成为国家稳定的基本要素。保护好网络是国家军事实力的体现。“这一点，业界显然已经达成共识。”

当然，现在安全业界对网络战的理解仍有分歧，“最终战况”仍众说纷纭，但翟胜军认为网络战的持久性决定了人们必须用发展的眼光看待这种“胶着状态”。他指出，网络建设的后期，不再是接入用户数量的比较，而是对网络信息源的贡献。美国目前的确是互联网信息提供的最大用户，但从另外一个角度看，中国的网民数量还在上升，无论是信息的产生与提取，还是信息的检索与利用，中国都将是最大的市场，尤其是 Web2.0 互联网交互技术，让网络变得更简单、更容易。“启明星辰的观点是：未来世界看发展，网络面前人人平等。”

制信息权是信息化战争的核心

当人们对网络战做进一步分析时，不少人将制信息权看作是信息化战争的核心，对此翟胜军深表赞同，他认为制信息权已经成为制海权、制空权、制太空权后，现代战争中指挥官关心的核心问题。

他首先解释了对信息权的理解：信息控制权应该是指战争中对通信系统的控制，在信息化时代的今天，还应包括国家基础设施控制网络与互联网。控制权表现为保护自己的信息不被敌方窃取和篡改，我方的指挥、控制系统不会受到敌方的干扰；同时能够有效利用对方信息。

“信息不同于其他产品，在数字化的世界中，信息表现为无介质性与时效性。无介质是指信息被读取或拷贝后，信息本身看不

翟胜军　信息安全专家

翟胜军，北京启明星辰信息安全技术有限公司政府行业首席信息安全专家。1994 年获得北方交通大学计算机专业硕士，先后从事软件开发、工程项目、产品技术等多项管理工作，有多年的网络厂家工作经验。2007 年进入信息安全领域，专业从事安全技术与市场研究工作，先后参与了运营商、政府、金融、军队等多个大型网络的安全规划与实施，有着丰富的实战经验。理论方面，提出了网络安全保障建设的参考模型——“花瓶模型”，为网络安全建设提供了一个可实施的、清晰化的安全建设架构。同时，对网络隔离、黑客攻击技术等方面有较多的探讨。

到任何变化，只有等到泄密后结果显现才被发觉；时效性是指得到信息的时间要合适，太早了对方可能改变，太晚了就可能失去应有的价值。”方寸之间，对信息的把握绝对不能马虎。翟胜军告诉记者，之所以这些信息的重要性高于其他战争武器的使用，是因为有了这些信息可以指导人们做什么、不做什么、多做什么、少做什么，知己知彼，就掌握了战争的主动权。实际上，信息控制权等同于控制战争进程发展的钥匙，所以，从打赢战争的角度讲：控制信息权和拥有善战的军队同样重要。

制信息权的重要性，可以从两个方面来理解：

一方面，人们已处于高度网络的时代。目前，互联网将发展到物联网的时代，网络成为社会各种要素的连接者，互通的标准与协议是开放的，所有的决策依据与控制命令都通过网络，信息的传递无所不在，信息战不只是战前收集信息，而是入侵对方“后方”系统的“尖兵”，过去是间谍，现在是黑客。网络入侵成为现代战争中必不可少的新型攻击武器——直接攻击对方指挥“神经”的特种部队。

另一方面，现代战争的新特点。现代战争中，攻击武器威力强大，双方使用起来都非常谨慎，往往在真实“空间”战争开始前先开始信息化“交战”。在没有“硝烟”的战场上，迷惑、扰乱、甚至剥夺对方指挥官的“指挥权”，为己方提供优势的战争地位，从态势上彻底摧跨敌人，成为信息战的重要目标。因此，信息战的较量，往往直接成为后续战争的方向标，掌握信息的控制权不仅赢得战争的主动，还可以真正做到“不战而屈人之兵”。

掌握信息的控制权，不仅可以提高赢得战争的机会，而且可以避免战争的实际发生。

人才决定战争的输赢

意识到了信息对网络战的重要性还不够，网络战比拼的最重要的就是实力。对此，往往有人认为网络战需要的实力就是技术，只要技术先进就能战无不胜。翟胜军对此并不赞同，他告诉记者，仅靠技术去打网络战还是远远不够的，网络战的核心是人才战。要具备网络战的优势，就必须具备培养网络安全人才的合适环境，建立人才培养的长期机制。

他坦言，国内目前在入侵检测、漏洞利用、木马创新等技术上都还很落后（从黑客工具的编写上很容易看到），提高技术不仅是依靠国家科研部门的高投入，更多的是实战经验的积累，网络安全人才的培养是关键所在，没有后备人才的保障，即使偶尔技术上的领先，也会很快被超越。

然而，网络战人才的培养与普通网络人员的培养不同，需要发散思维、逆向思维的人，规范化的教学体制下很难培养这样的人才。“因此，建立中国自己的、开放的网络安全实验室，建立民间的、自由的开源社区，营造一个社会型的、网络安全人才实战的培训环境，是赢得未来网络战争的基础要素。”

网络战的范围在延伸

在翟胜军的观点里，网络战不仅仅指的是国家间的对抗，那是比较狭义的网络战。他认为随着网络应用的普及与网络连接的延伸，网络战的范围也应当延伸出去。尤其是 2009 年兴起的“物联网”技术，不仅人们生活、工作越来越依赖网络的畅通，而且民生服务、政务管理等逐步数字化、网络化，跟百姓日常生活有关联的如国家电力、城市交通、铁路、民航、金融、通讯等都采用全国性的网络来管理，若被黑客入侵或攻击，不仅使这些企业会瘫痪，而且直接影响到百姓的生活与工作，同时国家也必然陷入恐慌与瘫痪。对国家安全的影响非同一般。

他举例说，美国连续几次的信息战模拟演习，如“爱因斯坦计划”，都是通过假想敌攻击美国的电力、交通、航空等基础设施开始的。令人欣喜的是，我国目前对网络安全非常重视，国家对重要的国家门户、重要服务都重点进行安全保障，奥运期间的奥运网络、公务员报名考试的网站、高考学生的查分网站……

“网络把个人、企业、国家联系在一起，网络安全不仅仅是国家管理互联网，而是涉及每个企业、个人的大事情。曾经有人戏言是网络让地球上的人拉近彼此的距离，地球村诞生了，全球经济一体化了；而网络也成为所有人、所有团体的神经系统，大家的疼痛也彼此相通。西藏一个小孩跌倒了，可能让上海的人感到疼痛。”翟胜军认为这并不算夸张。

用“红绿灯”管理网络

在采访的最后，翟胜军强调，要想赢得网络战，就必须先深刻理解网络的特性。一个有效管理下的网络，不仅拥有强大的抵御能力，也拥有强大的防护实力。他认为，网络世界最大的特点不是连通，而是开放。但没有限制的开放就意味着不安全，因为什么样的人都可以上互联网，不仅有美国政府，还有本·拉登的代言人，有天真的小学生，也有游戏赌徒。

“只有在网络中建立了良好的防护措施，保持网络的‘清洁’，才能把网络威胁消弭于无形。不能说网络都是不安全的，应该说，没有管理的网络是不安全的。比如城市的交通，没有交通警察前是无序的，冲突时常发生，有了红绿灯后，就变得有序了，虽然还有交通事故，但人们开始适应交通管理了，这就是管理带来的有序。”翟胜军也表示，目前的网络应该说可以达到人们对安全的需求，人们可以放心地使用，没有“因噎废食”的必要。“安全总是相对的，是否被攻击是看攻击你可以获得多少利益，没有利益的事情，攻击者也同样没有兴趣。”

在对网络战的定义做了扩充之后，翟胜军针对网络上的多

（下转第 16 页）

这一点 IBM 讲得很好，提出了“智慧地球”，“框计算”也属于这一层，怎么让计算机管理更智能化；第五层是顿悟。

百度对“框计算”概念和功能的描绘

翻开百度搜索，近期有关“框计算”（Box Computing）的内容越来越多，在谈到其概念时是这样描述的：框计算是 2009 年 8 月 18 日，百度董事长兼首席执行官李彦宏先生，在主题为“从你开始，创新世界”的 2009 百度技术创新大会上所提出的全新技术概念（http://baike.baidu.com/view/2735333.htm?fr=ala011.）。会上，李彦宏还描绘了“框计算”平台理念和前景构想，他表示“框计算”是为用户提供基于互联网的一站式服务，是一种最简单可依赖的互联网需求交互模式，用户只要在“框”中输入服务需求，系统就能明确识别这种需求，并将该需求分配给最优的应用或内容资源提供商处理，最终反馈给用户相匹配的结果。

未来，打开电脑或其他任何终端，桌面上只有一个简单的“框”，用户往“框”里输入想要的内容，“框”就能自动识别需求，然后在互联网可选范围内自动匹配满足用户相关需求的最佳应用和服务。李彦宏谈到的“框”，不再仅仅是指一个简单的用户 UI（User Interface）界面，也不是独指百度的‘搜索框’。

专家高调畅谈“框计算”影响

CNET（中国）媒体总编刘克丽认为，过去中国互联网及 IT 业界的发展理论都是以外国公司提出的技术理念为基础的，并影响着中国互联网产业的发展。而今天，很高兴看到我们中国 60 后的企业家提出了“框计算”这样一个对市场及整个互联网行业都会产生深刻影响的技术理念。无论是与 IBM 的“智慧地球”相比还是和谷歌的“云计算”相比，“框计算”理念更加前卫，更符合中国 4 亿多网民的诉求。更让人兴奋的是，在李彦宏提出“框计算”理念后，李一男、叶鹏等百度高层又基于“框计算”理念详解了百度对于这一技术理念具体所做的工作，告诉了大家如何能够更好地去实现它，而这是“云计算”、“动成长”等技术理念都不曾做到的。李彦宏的“框计算”听起来很朴实，但我相信，未来它终将改变所有的终端界面。

互联网专家刘兴亮则表示，李彦宏提出的“框计算”理念让我感到非常震撼，它代表了搜索引擎未来的发展新理念。一个框里面无所不在，一个框无所不能，它将引领未来互联网甚至各个行业的发展趋势。记得上小学的时候曾经有一篇科幻课文，说的大概意思是将来图书馆里一大屋子的书都可以装在一个像一分钱硬币大小的芯片里，当时虽然感觉十分好奇，但对其能否实现还是半信半疑，也难以想象得出。但是仅仅事隔十几年，我们对这种技术的实现已经不足为奇，也很容易理解。也许在科学领域，只有想不到，没有做不到。

不管怎么说，“框计算”都是值得肯定和探索的，至少是有了中国人自己的理念和想法。

（上接第 13 页）

种风险，将总攻击目的分成 3 类：

① 国家利益的攻击：这种攻击的目标是控制与破坏，形式很多，黑客、木马、病毒、DDoS、厂家后门等；

② 商业利益的攻击：获取企业间的商业利益是目的，一般是盗取而不是破坏。如商业机密的盗取、设计资料的获得、企业老板电话的录音；

③ 个人利益的攻击：主要是金钱的获取或针对具体人的报复。如盗取 QQ 口令、银行密码、游戏装备等，也有恶意中伤的消息发布，如爱滋女事件、人肉搜索等。

从攻击的技术上与方法上对网络威胁分类就更多了，翟胜军从用户体验角度上分出以下几种类型：

① 感染性的攻击：病毒传播无孔不入，典型的是木马通过病毒大量传播，获取被攻击者信息与控制权后，上报给攻击者管理者，把用户计算机变成“肉鸡”，用户在网上冲浪、聊天、收发邮件时不知不觉中被“感染”；

② 直接攻击：用户的资源价值很明显，黑客直接瞄准用户入侵，这类目标一般是公众网站、企业门户、金融控件等，攻击的技术很复杂，如漏洞攻击、密码破解、SQL 注入等；

③ 野蛮攻击：主要的目标是破坏、中断服务，典型的是用 DDoS 方式攻击政府门户，或游戏、视频类等商业网站，直接让对政府造成网络服务中断，或要挟服务方付钱买单；

④ 隐藏攻击：目标是监控用户计算机行为，这在国家网络战之中很常见。在需要的时候盗取密码，或控制目标对象的机器。这种攻击的目的很多，大到为国家信息化战争准备的厂家后门，小到木马产业链建立的收集渠道，都是无声无息的，隐藏在目标对象的计算机（也许是手机、智能终端等）内。

在采访结束时，翟胜军谈到，虽然网络战已经初露锋芒，但国内网络安全目前仍处于基础建设时期。在经历过网络建设、应用开发、数据集中、存储整合等 IT 建设大潮后，网络内容丰富起来，虽然人们日益体会到网络安全的重要，但人们对安全的认识还比较初级，很多人认为“防火墙 + 防病毒”就是网络安全，对监控与审计也很陌生，还没有认识到体系化的安全措施、完善的安全管理的效能。随着国家等级保护标准、涉密分级保护标准的颁布，开始对涉及国家重要基础设施的网络系统强制性保护，人们将逐渐加深对网络安全的理解。