【前　言】本刊“网络战”专题已经进行到第四期(采访中科院许榕生研究员——2009年9期;采访国防科技大学计算机学院网络与信息安全研究所龚正虎教授——2009年10期;采访浙江省信息安全协会安全服务委员会范渊主任——2009年11期)。本期专访记者约请到北京理工大学信息安全与对抗技术实验室主任罗森林教授,罗教授提出的“网络战不仅指国家层面的对抗,目前已经与日常技术交融。网络防护重点在平时,网络战是不知不觉中的战斗,矛和盾都要研究”等内容给了我们很多启示,在此对罗教授表示由衷感谢。

和平时期的网络战

——北京理工大学罗森林教授谈网络战背景下的网络攻防

罗森林

北京理工大学信息安全与对抗技术实验室主任

1968年生,男,博士,教授,博导,北京理工大学信息安全与对抗技术实验室主任、专业责任教授,研究方向为信息安全、生物信息处理、媒体计算等。已发表学术论文50余篇,出版著作4部,出版译著1部,获发明专利2项、实用新型专利1项,负责或参加完成国家自然科学基金、国家科技支撑计划、国家863计划、国家973计划、国家242计划、北京自然科学基金、博士后基金等省部级以上项目20余项。作为第一负责人负责教改项目包括教育部高等学校特色专业建设点,北京高等教育特色专业建设点,国防特色目录外紧缺本科专业“信息对抗技术”建设点等。此外,作为主要人员之一参与国家信息安全专项规划、信息安全等级保护,以及某部重点信息安全项目等工作。

本刊记者　胡晓荷

防护重点在平时

“5·12”汶川地震时,当所有的通信系统都宕了的时候,比较原始的手摇发电机却起了作用,这给了我们不小的启示,也让我们对日常所依赖的各种网络系统产生无限深思。

本期网络战专题采访过程中,北京理工大学信息安全与对抗技术实验室主任罗森林教授表示,目前网络战不仅是指国家层面的对抗,网络战的技术内容已经与日常生活中的技术交融。

罗教授表示也曾经对网络战本身的概念仔细分析过,按大家常规来理解,更多可能指的是计算机网络战,个人认为网络战不应仅仅是局限于计算机网络。网络战可以理解为,基于攻防双方信息安全的防御、发现、应急、对抗能力,利用网络和网络技术的信息安全防御、攻击检测、攻击的行为和对抗过程,其网络涵盖计算机网络、移动通信网络、广播电视网、军用通信网及其他各类网络。当然,从全球来讲也在不断出现新概念,概念本身并不重要,重要的是内涵。现在信息发展是非常快的,从国家跟国家的战争来讲本征的属性就是对抗。从制信息权的角度,“制”就是要“知道”,如果“不知道”,想取得胜利简直是不可能的,因而“制信息权”是非常重要的、而且是最重要的。在现代信息科技快速发展过程中会带来更多的安全问题,那么这些安全问题成为“事件”以后造成的后果越来越严重。信息对抗也好、信息攻击也好,都是各个国家要努力提高的能力,没有必要避讳。”另外,我认为安全防护重点在平时,而不是真正发生战争的时候,事实上是在平时不知不觉中的战斗。”罗教授说道。

网络攻击的特点

谈到网络攻击的特点,罗教授表示,低成本、效益大,从某种角度上讲要求高技术水平,但从另外一个角度讲技术要求也不一定高,比如黑客的技术也在发生变化,以前要求黑客的技术水平很高,现在可以直接利用网络上的黑客工具(如扫描器)去实现攻击。从效果与后果的角度讲,以前的网络攻击主要是出于好奇,以展现、炫耀为目的,现在已经涉及到政治、经济、文化和国防,如果破坏网络中的某些关键设备,如核心路由器、核心交换机等,就会造成大面积的网络瘫痪。目前,手机上网越来越多,手机病毒、手机诈骗都已出现并越来越多,移动通信网络也在慢慢发生着变化,也需要有监控,攻防也在做。网络电视、网络视频、网络购物等也越来越多。网瘾问题也比较严重,有的学生一旦网络上瘾很难纠正。罗教授认为这也是网络战的一部分,对人的心理、精神的影响非常大,可以说网络攻击的形式多种多样。网络战在和平时代会表现出以上这些特点。

网络安全防护非常重要和紧迫

目前网络的安全事件已经非常多,因此网络防护显得非常重要、非常紧迫。网络攻击形式层出不穷:窃密、摆渡木马,还有各个国家目前都在发展的蜜罐技术、僵尸网络,老

百姓比较常见的电话诈骗中有很多也都与互联网相关。“前些年，学校曾经授权我评估校园网的安全性，当时发现安全问题太严重了，通过多年的发展，现在的安全状况要好得多了。”罗森林教授说道。

理工大学最早在2002年就提出校内信息安全与对抗技术竞赛，主要是考察计算机网络这一部分内容的。这一点的提出在国内也是比较早的。经过几年的努力，该项竞赛成功走向了全国，并于2008年推出了第一届全国大学生电子设计竞赛——信息安全技术专题邀请赛，本届竞赛产生了比较大的影响，全国有40多所重点院校参与。罗教授介绍到，这一竞赛最开始仅是对8个知识点的考察，而在2009年的知识竞赛中，考察的信息安全与对抗技术知识点已经达到90个，包括网页木马、漏洞利用、社会工程学(或社交工程学，即利用被攻击者熟人的关系网套取诈骗信息)、脚本技术等，通过模拟真实网络中的动态攻防过程，达到实践网络安全技术、共创网络安全环境，提升学生的实践能力、普及安全常识、探讨更高端的技术目的。并且组织形式是靠学生的自主设计、自主参与，近年来大一大二的学生占主力，这说明学生的技术水平都在普遍提高。现在全国有70多所院校有信息安全专业或者信息对抗技术专业，教育部批准理工大学建立信息对抗专业是在1998年，当时国内只有4家学校有这个专业。而短短的几年时间，目前各个大学基本上都有了信息安全专业，这说明国家对信息安全的重视以及信息安全本身的重要。国家在十一五规划中专门提出信息安全项目，国家自然科学基金、863项目中都有信息安全计划。

网络战本身在不断发生着一些变化，范围目前也在不断扩大，涉及到的领域也越来越丰富，包括日常生活和各行业领域。网络攻防的过程永远不会完结。

都有哪些解决措施

罗教授表示，分析一些泄密事件，会发现之所以有这么多安全事件的发生，说明光靠技术是不够的，更需要人们安全意识的提高。目前有些现象说明安全意识没有、安全常识不足，有些人就根本不想电脑里存的是涉密信息。

那么如何防范呢，首先要不断提高安全意识和安全常识，另外，也不要忽略实体的安全问题，技术安全防护做得很好，可是电脑或手机被人家偷去了，什么也都不安全了。这往往容易被忽视。

还要构建基本的防御体系。理工大学校内技术竞赛里面就有一个口号：“要实现网络安全技术，共创网络安全环境”。矛和盾都要研究，光研究矛不行，光研究盾也不行，我个人认为攻也不要避讳，就是要研究。如果光研究防，连攻的技术技巧都不知道，那我们怎么防？因此，要结合信息、信息系统、运行环境，构建综合防御体系。

此外，更要从理论层面去把握信息安全问题，构建信息安全的基础理论体系，目前信息安全角度的安全标准、自主知识产权、等级保护都在不断发展、不断完善，我们应该有一些信息安全领域的工程系统理论。罗教授在给学生上课的时候也会讲这一点，并且还出版了一本书——《信息系统与安全对抗理论》，已经讲了好几届。“我们目前已经构建了一套——信息安全基础层次、系统层次的原理和方法，例如，快速响应原理、反其道而行之相反相成原理、共其道而行之相成相反原理等。还有木桶原理——分析整个链条里面，哪个是最薄弱环节，防也是防薄弱环节，攻也是攻薄弱环节，怎么去防御？还有核心技术转移方面”罗教授介绍说，比如计算机加密方法，加密把密钥做得安全性很高，还可能会出现问题，因为关键不在于加密技术算法本身，而是密钥的持有者，比如锁很结实，但是钥匙丢了，很多人往往需要记密码，而有的人习惯于把密码放在电脑里，所以目前核心点已经转移到密钥的持有者身上。如果这些道理大家都懂，就不会单纯去强调密钥有多长，因为再长也记不住，最后要把密钥缩减到能够记住或者方便存储的地方，那么它的安全性转移到这里了，已经不是密钥算法本身了。这些技术核心措施转移构成串行链结构，形成“脆弱性”环节的概念。

网络战中制胜的关键不是一两句话、一项技术，需要从系统层面考虑，在某种程度上才能做到很好的防御，首先从技术来讲的攻防，攻的能力、防的能力，还有自主知识产权等问题，比如，前段时间某个国外品牌的新下线硬盘，本身就存在大量的恶意代码。如果我们有自主知识产权就可以避免很多问题。此外，攻和防不一定非要求技术很高，要善于用巧劲和规律去解决实际问题。信息安全理论要落到实处才能解决问题，仔细分析，目前社会上的问题跟网络上的问题映射关系是非常明显的，所以探讨网络安全问题可以从这个角度出发。在现实生活中发生的行为，一般在网络上也会出现，比如现实生活中有社区、沙龙，网络上也有，最近比较明显的开心网上的种花种菜、买房装修、炒股都反映出了现代生活中人们的心理追求。所以社会行为与网络行为可以对应着来研究。

关于使用无线网的安全防范

目前包括3G在内的无线网已经很普及，跟很多人的日常生活息息相关。无线网络确实存在很大的信息安全问题，那么怎么防范呢？罗教授建议：首先不要在电脑中存储重要信息，如账号信息；作为一般用户尽可能地加强必要的防范措施，如安装杀毒软件、及时打补丁、及时升级病毒库等；对计算机异常行为要尽可能感知；严格自己的上网行为，尽可能避免被植入或引人恶意代码等。