电脑黑客与网络战

李永田

（空军第一航空学院 信阳，464000）

摘 要：简述了黑客及其破坏作用，说明了黑客对敌方网络进行病毒攻击的手段，并利用敌方网络进行情报窃取、情报欺骗和信息轰炸的攻击方法。对网络安全的防护方法进行了探讨，对在网络对抗中采取何种应对措施提出了几点看法。

关键词：电脑黑客 网络战 计算机病毒 防火墙技术

随着网络技术的迅速发展和应用范围的不断扩大，未来战争敌对双方将围绕信息网络的安全进行激烈的对抗。如通过网络节点或链线侵入对方用于经济、军事目的的互联网络，窃取其政治、经济、军事情报，更改数据库，发布假命令，输入计算机病毒攻击网络软、硬件设施等。在信息网络上，黑客对网络的攻击活动越来越频繁，并且脱离了早期"电脑工程师"的侠客行为，甚至带有战争活动色彩。2000年2月上旬，美国8家著名网站相继遭到黑客协调一致地外来攻击，引起了全球各国的关注，迫使人们重新审视网络时代的安全性问题，更引起人们对网络时代信息战的警觉和对国家安全的关注。这说明网络战已无法避免，而黑客在网络战中可发挥其独特的干扰和破坏作用。

1 黑客及其破坏作用

黑客是英文"Hacker"的译音。以前，人们对黑客的定义是一个对电脑着迷的"工程师"，是一个出于个人兴趣、喜欢探人隐私，并对网络技术非常谙熟，以挑战固有规律为乐、具有冒险精神和恶作剧心理的反抗者。也有人形容黑客是信息战领域里的特种作战部队，是一伙手持"杀手锏"，专击"生死穴"，来无影去无踪的幽灵。通常情况下，黑客是指那些通过窃取密码而非法进入他人电脑或网络系统，修改网络路由、窃取机密信息、进行情报欺骗或向网络施放病毒等进行破坏活动的不速之客。

黑客的破坏作用涉及到社会生活的各个方面，例如闯入军用网络窃取敌方情报、通过银行网络非法转帐侵吞他人资产、通过邮电网络利用他人帐号偷打长途电话、发送大量信息炸弹使网站的网络服务设施瘫痪，给对方造成直接或间接经济损失。这种行为都属于黑客现象。在军事上，黑客可使对方网络系统瘫痪或感染病毒，也可向对方网络插入误导信息，影响或干扰对方的判断和决定。北约对南联盟实施空袭时，南联盟的黑客向北约计算机系统投送了大量的"爸爸"、"梅利莎"、"疯牛"等电脑病毒，每天集中大量邮件进行"电子轰炸"，最多的一天达到2 000多件E-Mail，致使北约布鲁塞尔总部的因特网服务器受到破坏，部分计算机的软件和硬盘遭到重创，系统功能大减。科索沃战争表明，电脑黑客拿起电脑病毒和"电子轰炸"这些利器，可以在以弱胜强、以劣胜优的战争舞台上大显身手，发挥其干扰和破坏作用。

2 黑客的攻击手段

在C⁴I系统中，计算机扮演着"指挥官"的角色，它的每一个命令，每一个数据的失误传送都可能产生不可估量的后果。而情报的获取、指挥中心与各部队之间的通信、指挥命令的下达、武器的控制都与计算机密不可分。也就是说，计算机和计算机技术已渗透到指挥、控制、通信、武器系统、电子战、信息战等现代化军事系统中，并成为未来军事战争的核心和支柱。如果能对敌方计算机实施有效地控制和破坏，无疑将起到事半功倍的效果，在这一点上，黑客能发挥其独特的作用。

黑客对计算机网络的攻击可采取多种形式，其破坏效果也十分明显。有的攻击方式十分简单实用，而有的攻击方式则需要电

收稿日期：2000-04-17

脑专业基础知识和最前沿的电脑尖端技术知识。总的来说，黑客的攻击方式可归纳为如下三类。

2.1 病毒攻击

病毒解释为“攻击性的致命信息源”(Vital Information Resources Under Siege)，用词首缩写词“VIRUS”表示。计算机病毒(Computer Virus，简称 CV)是能够侵入计算机系统并给计算机系统带来故障的一种具有极强自我繁殖能力的指令程序，它能够影响其它程序的正常运转及数据安全。计算机病毒将自身的复制品或变种传染到其它对象上，具有传染性；计算机在加载被感染的对象时，病毒乘机侵入系统，在未授权的情况下因具有一定的欺骗性而被加载，即具有欺骗性；病毒在发作前难以发现，具有隐蔽性；在发作后，删除或修改数据、占用系统资源、干扰机器运行，具有极大的破坏性；计算机病毒的代码很短、精巧不易引人注目，具有精巧性；计算机病毒侵入系统后一般不立即发作，而需经过一段时间满足一定条件后才发生作用，潜伏期长短不一，说明病毒具有潜伏性；计算机病毒即使在被发现的情况下，它所破坏的数据、程序和操作系统等也往往难以恢复，即计算机病毒的顽固性。从上述计算机病毒的特点可知，如果计算机病毒传染到整个网络，一旦符合病毒发作的条件，便可造成敌方整个指挥系统的瘫痪，短时间内无法恢复。因此，计算机病毒攻击是黑客对敌方常采用的方法之一，也是最有效的攻击方式之一。

黑客只要把病毒或带病毒的软件置于网络中，它将对一切可能攻击的目标进行攻击。目前黑客对敌指控网络注入病毒的方式有三种：

一种是间谍方式。黑客借助病毒软件工具，可以有针对性地频频对敌方网络发动袭击令其瘫痪，多名黑客甚至可以借助同样的病毒软件在不同的地点“集中火力”对一个或多个网络发动袭击，而且黑客们还可以把这些软件神不知鬼不觉地通过互联网装在别人的电脑上，然后在电脑主人根本不知道的情况下“借刀杀人”，以别人的电脑平台对敌方网络发起攻击。

第二种是芯片武器或“芯片陷阱”。黑客为达到预定的目的，对出售给潜在敌方的计算机芯片进行暗中修改，使之可遥控使用，美国黑客或黑客集团已开始研究芯片武器，并在出售给盟国和潜在敌国的武器系统中，使用经过改装的芯片，以起到“定时炸弹”的作用。例如在海湾战争中，伊拉克部分防空指挥系统由于购买了美军特工嵌入病毒芯片的打印机，其网络被遥控激活的病毒所瘫痪。

第三种是空间注入方式。黑客或黑客集团可以将计算机病毒转换为病毒代码数据流，并将其调制到电子设备发射的电磁波中，以无线电方式、卫星辐射式注入方式把病毒植入敌方计算机主机或各类传感器、网桥中，伺机破坏敌方武器系统、指挥控制系统、通信系统等高敏感的网络系统。

2.2 情报窃取及情报欺骗

指挥控制战主要是控制对方的决策方向，决策方向来源于信息，信息是决策的材料。决策的过程是信息收集、处理、加工、制作和产出(即决策)的过程。因此，信息可扰乱对方的分析判断。毛泽东对指挥员的决策过程作了这样的表述：“指挥员的正确部署来源于正确的决心，正确的决心来源于正确的判断，正确的判断来源于周到的和必要的侦察，和对于各种侦察材料的连惯起来的思索”。这个决策过程可以简化为如下思维模式：

侦察——分析——判断——决心——部署

信息获取——信息处理——信息确认——信息转化——决策

在竞争对抗活动中，任何一方企图实现影响和控制对方决策行为的目的，显然不可能通过直接指挥或支配对方的方式来达到，而是通过信息诱导来实现。信息诱导是手段，使敌方作出有利于己方的决策是目的。目前，军事上信息的获取，主要是利用照相侦察卫星、电子侦察卫星、无人侦察飞机、地面电子侦察站和间谍人员等手段来实现。

从网络防御的角度讲，黑客虽是一个挥之不去的梦魇，但从网络进攻的角度而言却恰恰相反，他可以对敌实施有效的攻击。黑客的出现立即引起了军界的广泛关注，这是因为，黑客从网络上获取的信息及情报比较真实，并且方法灵活，手段隐蔽，安全可靠，不需要投入大量设备，目标小又不易被发现。黑客们一旦通过有效途径掌握敌通讯口令进入指挥系统，就可冒充合法用户，获得真实有价值的信息，对敌实施情报窃取以利于知己知彼。1997 年 6 月间，美国国家安全局举行了一次代号为“合格接收者”的秘密演习，参与者是信息战“红色小组”，另外还雇佣了 35 名黑客，任务是设法闯入美国本土及统率 10 万大军的美军驻太平洋司令部使用的计算机网络。演习结果使美国国防部的高级官员深感震惊，几个“黑客”小组 4 天之内就成功闯入了美军驻太平洋司令部以及华盛顿、芝

加哥、圣路易斯和科罗拉多州部分地区的军用计算机网络，并控制了全国的电力网系统，而且黑客们实际上挫败了几乎所有跟踪他们的努力。美国联邦调查局和国防部都试图找到“黑客”，但只发现了其中一个小组。演习结果表明：一个装备、技术都不太复杂的敌人，以少于30人的队伍和数量不足的资金，就可以给防御不足的系统造成相当大的损害。因此，黑客们通过计算机、调制解调器和电缆接口，使用一些在网络上唾手可得的软件，就能轻易对敌计算机网络进行大规模的破坏活动——有鉴于此，在未来的指挥控制战中，电脑网络战将是基本战法之一。

在进行情报欺骗时，黑客们可以在网上发送大量的不可靠、不相关、模棱两可、互相矛盾的信息，伴随着真正有价值的信息来迷惑敌方，使对方决策人员在信息过剩、信息超载、信息盈余、信息膨胀的条件下，无法确定什么是虚假信息，什么是有价值的信息，扰乱对方决策者的分析判断。信息愈多，指挥员对其综合的难度就愈大，下决心愈难。信息愈多，在有限的时间内作出决定，判断的主动性就愈大，准确性愈差。所以，情报欺骗可使敌方作出有利于己方的错误决定，甚至造成敌方的误会而互相残杀，达到不战而胜的目的。

2.3 信息轰炸

传统的黑客行为一般是侵入型为主，通过窃取密码进入系统，造成破坏。这类黑客往往具有比较高的技术背景，而防备完善的系统，可以通过更高级的技术手段捕捉到黑客，或将其阻挡在系统之外。但在目前的互联网上，许多网站遭到的袭击都是一种技术手段非常简单的方式——信息轰炸，黑客根本不入侵网站，而是用大量的信息炸弹使网站的网络服务瘫痪。这种方法几乎不需要技术背景，也就是说，任何人都可能成为网络攻击者。任何个人只要拥有一台计算机和入网线路，不受时间、地点、国籍、党派的限制，都可以上网调阅、发布、传递信息，都可以攻击装有芯片的系统和进入网络的军用和民用装备，并且极难控制。所有这些，为任何个人或团体实施网络攻击提供了客观条件。

黑客进行信息轰炸时，攻击的手段既简单又实用，具有以下特点：利用网上的计算机和入网线路，通过网上的一些公开软件进行操作；在攻击方法上如出一辙，主要是通过多个地点同时向被袭击的网站发送很短的信，由数个通道同时不间断地发送，由于信很短，进来的速度非常快，量很大，使其超出网站自身的负荷能力而整批拒绝服务；攻击的行动隐蔽，不留任何踪迹，很难找出黑客来自何方；攻击效果十分明显，通过这种极其简单的方法可让一个投资巨大、技术十分先进的网站在1s内遭受重大经济损失。

3 网络对抗

3.1 网络安全

网络安全问题是一个涉及网络系统本身和网上信息、数据安全的综合性问题。作为现代战争指挥控制系统核心设备的计算机系统，如果缺少应有的防护，则极易受到“来自鼠标和键盘的攻击”，并且不受国界、军民、和平与战争等因素的限制。针对网络被黑客攻击的状况以及黑客攻击所采取的手段，建立计算机网络安全体系是一个非常现实、非常紧迫的课题。首先，应制定严格的网络安全法。将计算机及其网络技术的开发、应用、管理、安全等问题法律化，以法律手段保障计算机网络的安全。其次是开发相应的防护技术。防护技术是实现网络安全最有效的方法，为保障网络安全应着重开发密码技术、防火墙技术、鉴别技术、计算机网络病毒防治技术、信息泄漏防护技术、计算机网络安全薄弱环节检测技术等等。

3.1.1 密码技术

计算机用户都备有密码口令，在使用机器时，输入自己的口令，准确无误后再开始使用机器。由于某种原因，用户可能输错自己的密码，但一般不会连续出现多次，而黑客要得到密码口令进入计算机系统，常使用试探法，需要连续不断地尝试。为此，可以编制一种程序，当发现有人多次输入错误的密码时，能自动记录此人的电话号码或自动报警。为防止黑客进入计算机系统，口令的设置应仔细斟酌，不要简单地用与人名、生日、音乐、午餐、动物、蔬菜等有关的名词作口令。口令的设置应该是容易记忆，难以猜测，经常改变，最好用字母和数字的组合。

3.1.2 访问控制技术

黑客一旦得到密码进入计算机系统，就可获得计算机系统内的所有数据。为防止利用计算机行窃，在设计计算机系统时，设置一些关卡，使用户只能查阅和使用与自己有关的资料和数据。

3.1.3 防火墙技术

防火墙是阻挡外部网络影响内部网络的屏障。外部网络无论如何攻击，有了防火墙的设防与把守，内部网络就可高枕无忧。而网络防火墙的设置，需要网络决策人员及网络专家共同决定本网络的安全策略，即确定什么类型

的信息允许通过防火墙，什么类型的信息不允许通过防火墙。防火墙的作用就是保障本系统的安全，对外部网络和内部网络交流的数据进行检查，符合标准的予以放行，不符合标准的拒之门外。

3.1.4 鉴别技术

在计算机系统中，时时刻刻都进行着各种各样的信息交换，从安全的角度考虑，必须保证交换过程的有效性与合法性。鉴别技术就是保证信息交换过程合法有效的一种手段。鉴别技术主要有：报文鉴别，身份鉴别，数字签名。

a. 报文鉴别。报文鉴别是指在两个通信者之间建立通信联系之后，每个通信者对收到的信息进行检证，以保证所收到的信息是真实的过程。检证过程必须确定报文是由确认的发送方产生的，报文内容没有被修改过，报文是按与传送时的相同顺序收到的。

b. 身份鉴别。身份鉴别一般涉及两个方面的内容：一是识别，一是验证。所谓识别就是对系统中的每个合法用户都有识别能力。为保证识别的有效性，必须保证任意两个不同的用户都不能具有相同的识别符。所谓验证就是指在访问者声称自己的身份后(向系统输入他的识别符)，系统还必须对他所声称的身份进行验证，以防假冒。识别信息(识别符)一般是非秘密的，而验证信息必须是秘密的。验证方法有四种类型：验证他知道什么(口令等)；验证他拥有什么(通行证等)；验证他的生物特征(访问者的指纹等)；验证他的下意识动作的结果(访问者的签名等)。前两种方法验证系统简单，但安全性差。后两种方法安全性高，但验证系统复杂。

c. 数字签名。信息的收发双方如果对信息的内容及发送源点没有什么争执，只采用鉴别技术就足够了。因为鉴别技术可以保证在信息传送的过程中对信息内容的任何改动都可以被检测出来，并且能够正确地鉴别出信息发送方的身份。但当信息的收发双方对信息的内容及发送源点产生争执时，就应采用另一种安全技术——数字签名。数字签名要达到如下效果：在信息通信的过程中，收方能够对公证的第三方(可以是双方事前同意委托其解决某一问题或某一争执的仲裁者)证明其收到的报文内容是真实的，而且确实是由那个发送方发送过来的，同时，数字签名还必须保证发送方事后不能根据自己的利益来否认他所发送过的报文，而且收方也不能根据自己的利益来伪造报文或签名。

3.2 网络对抗

首先，要增强网络对抗意识，研究网络对抗理论。在网络对抗中能力弱的一方，必将遭受优势对手的强大攻击，从而导致大量政治、经济、军事情报泄露，经济、军事信息系统遭受破坏，经济活动陷于停顿，社会发生混乱，指挥作战失灵，最终不得不在政治上妥协。为此，应根据信息网络对抗的特点，对己方网络要采取相应的防护措施，并加强网络对抗的电磁摧毁、结构破坏、病毒袭击、网络渗透和网络保护等方面的研究。应加紧制定网络发展战略，加速发展网络战技术和攻防技术，以提高网络对抗能力。

其次，建立网络作战体制。网络对抗是系统对系统的对抗，军队、政府甚至企业都将卷入其中，几乎是全社会参与，因此，必须要有统一的机构来领导、协调各方面的力量，制定统一的作战计划，采取一致的作战行动，建立以军队为主，支持和保障多层级、覆盖全社会的、高效的网络对抗指挥机构。

第三，培养网络作战人才。在未来的信息网络对抗中，人的因素仍是第一位的，网络的管理、操作、维护，网络进攻和防护技术的研究，对抗中的战略、战术运用等，都需要高素质的网络人才。从军事角度上讲，黑客并不是单纯的搞恶作剧或泄私愤的反抗者，他的作用提醒我们：要培养自己的黑客，使己方的黑客不仅能够随时向敌方网络发起有效的攻击，而且要能够保护己方的信息网络安全，以便在网络对抗中争取主动。未来作战，无“网”不胜。网络战需要专门从事网络对抗研究的计算机专家队伍，需要懂得网络对抗技术及战术的指挥员队伍，需要具有一定计算机及网络基础知识，并具备一定特殊技能的网络战士。

4 结 束 语

网络对抗是黑客与反黑客的对抗。在网络对抗中，黑客将是一支重要的作战力量。要想在网络战中立于不败之地，就必须顺应时代发展的需要，从现在起，把网络对抗技术摆在战略高度，努力发展网络技术、战术，培养自己的“网络勇士”，研制自己的“网络武器”，构筑自己的“网络国防”，铸造网络的坚盾利剑。

参 考 文 献

1 黄淑申．电脑黑客的研究意义及对抗效果．火力与指挥控制，1999，(4)

2 陈爱民等．计算机的安全与保密．电子工业出版社，1992

3 何江安等．计算机病毒防治实用教程．清华大学出版社，1990

4 毋笃强等译．计算机病毒防护．兵器工业出版社，1990