21 世纪战争新概念——网络战*

陈洪超, 段本钦, 李 涛
(总参通信部驻天津地区第 1 军事代表室, 天津 300140)

摘 要: 在 21 世纪, 信息已成为军事斗争的重要资源, 而集结了大量国家和军队信息的网络, 将与信息时代战争的主动权同等重要, 将成为信息战争作战理论研究的重心。文中立足于打赢未来战争, 计算机技术和现代通信技术在军事领域广泛应用的前提下, 主要介绍了网络战的重要地位、主要特点, 对战争的破坏性乃至对整个战局的影响, 在进行网络战时所采取的多种手段, 网络战的关键技术以及网络安全的防护问题, 从而引起人们的思考, 在和平时期如何预防未来的网络战, 怎样积极地准备网络战, 以便在未来的高科技战争中防范敌方的网络袭击, 采取行之有效的攻击方法对敌方的通信网络予以沉重打击, 使我军在战争中占有主动, 从而夺取整个战局的胜利。

关键词: 网络战; 重要地拉; 主要特点; 网络技术; 安全防护
中图分类号: TP393 文献标识码: A 文章编号: 0032-1289(2001)04-0073-04

New Concept of Wars in 21st Century——Network War

CHEN Hong-chao, DUAN Ben-qin, LI Tao
(1st Military Representatives Office of Communication Division of PLA General Staff Headquarters in Tianjin, Tianjin 300140, China)

Abstract: In the 21st century, information will become the crucial resource in military campaigns. At the same time, the network that integrates much state and army information will be of the same importance as having the initiative in the campaigns in information era, and the former of which will become the focus of theoretical study of campaigns in information era. Starting from how to win the war in the future, this paper mainly introduces the important role, main features, its destruction to the war, its effect to the general war situation of the network campaigns, the various methods that should be adopted in network compaigns, the key techniques of network and the issue of network security under the precondition of wide application of computer technologies and modern communication technologies. It intends to arouse people's thinking about how to prevent the network campaigns, how to actively prepare for the network campaigns in peaceful time so as to guard against the network attacks by the enemy, take effective attacking actions to seriously destroy the communication network of the enemy, and enable our army to have the initiative in the war and win the whole war.

Key words: network war; crucial role; main characteristics; safety protection

网络战, 是敌对双方针对战争可利用的信息和网络环境, 围绕"制信息权"的争夺, 通过计算机网络, 在保证己方信息和网络系统安全的同时, 为扰乱、破坏与威胁对方的信息和网络系统以取得战争的最后胜利而展开的对抗活动。网络战属于信息战的范畴, 是信息战的一种重要形式。信息战是指为了获取信息优势, 通过影响敌方信息、以信息为基础的过程、信息系统和计算机网络, 同时保护己方信息、以信息为基础的过程、信

* 收稿日期: 2001-08-31; 修回日期: 2001-09-25
作者简介: 陈洪超(1974-), 男, 学士, 工程师.

息系统和计算机网络而采取的各种作战和行动。作为世纪之交的一种全新的作战模式, 网络战在 1999 年的科索沃战争中已显示神奇的软战魅力, 受到各国军事专家们的广泛青睐。21 世纪将是网络战的世纪。

随着计算机技术和现代通信技术的飞速发展以及在军事领域的广泛应用, 敌对双方将很大程度上依赖于绵密的各种信息网络运转他们的战争机器。未来战争的胜负已不再取决于谁在战场上投入资源的多少, 而取决于谁对战场的 "制信息权 "掌握的好坏。对信息权的控制程度, 将直接影响到对有限人力、物力资源运用的效能。而所有信息的收集、传递和加工处理等都离不开计算机网络系统, 它是网络战的焦点。敌对双方通过破坏对方计算机系统的软、硬件资源, 力图扰乱、削弱、瘫痪敌方的武器系统、控制系统、决策系统, 造成敌方信息控制系统的紊乱、通信联络中断、指挥失灵、武器失控、秩序混乱, 使敌方军队的指挥官决策失误, 军队丧失战斗力, 为夺取战争的最后胜利创造有利条件。

1 网络战的主要特点

1.1 军民网络融合是必然趋势

计算机技术和通信技术的迅猛发展, 使网络覆盖面日益扩大, 将全球数以亿计的计算机都网罗进了网络世界。四通八达、纵横交织的全球互联网络, 不断将更多的军用与民用计算机系统联为一体, 军用信息资源已经开始融入社会网络系统; 同时, 民用信息资源也不断地向军用网络渗透。军民网络之间通过各种电话、电报、图象、数据网络建立了千丝万缕的联系, 从而正在形成一个没有国界之隔、没有网民身份之分的网络世界和 "网民皆兵 "的网络空间。可以预料, 今后军事领域的抗衡, 一定会波及到这个网络空间, 并扩展成为整个社会系统的全面抗衡和较量。任何掌握网络传输技术、精通计算机知识和先进的编解码技术的机构或个人, 都可能成为一名 "网络战士 ", 在网络战场上一显身手。作战双方通过发动网民, 可以在全球任意有网络互联的位置上于任意时间部署自己的 "网络战士 ", 对敌方网络系统展开攻势, 进入敌方多层加密的网络系统, 对敌方各种领域内的计算机系统、入网设备或数据库进行渗透、修改, 窃取其网络系统内部及数据库关键资料, 截取或扰乱敌方对重大国计民生系统和军事指挥系统的指挥控制权, 破坏其指挥中枢和武器系统, 实施隐蔽或公开、跨国界、超越传统战争理论的崭新的网络战, 最大限度地容纳各种人员在各种环境下随时随地对敌作战, 达到一般作战方式不可能达到或不能迅速达到的预期作战目的。

1.2 网络战具有广泛性

网络战具有实施范围、实施时间、实施人员、攻击目标的广泛性。一是作为连接军事与民用各行业与各领域的计算机网络, 有着广阔的覆盖空间, 同时由于网络信息交流和网络资源相互利用的需要, 很难对其加以限制和约束; 二是每一个体, 在世界任一角落, 都可以极其隐蔽地利用因特网站进行破坏活动, 而攻击手段并不复杂; 三是参与网络战可以有多种途径, 且花样繁多, 包括利用公众电话网、各种专用数据网、贸易手段、派遣敌特攻击等, 而接入网络的媒质却可以是有线、无线或光通信系统等常用通信手段; 四是实施网络攻击的时间可以在公开敌对的时期进行, 也可以在战前、战中秘密进行; 可以间断或按规定的时间进行, 也可以每天每时不间断地进行, 极其灵活。组织良好的网络先机攻击, 或许可以促成 "不战而屈人之兵 "的最佳效果, 使军事实力相对弱小的国家避免失败; 五是网络攻击发起的地点可以在战区内, 也可以在战区外; 可以在本国国土上, 也可以在敌国国土上, 或世界任何一个有网络连接的地方; 六是参战人员可以是军事人员, 也可以是非军事人员、网络专家、网络爱好者; 七是网络攻击与防护的目标不仅仅是军事网络本身, 它还覆盖今日之金融网络、商贸网络、交通网络、电信网络、科研网络等各种信息应用领域, 任何国家尤其是发达国家在这些 "网域 "内存在着巨大的经济、政治、军事利益。近几年来发生的网络病毒泛滥和网络黑客破坏计算机系统的许多实例已经证明, 这些网域是最易遭受信息攻击的领域, 并越来越引起军事家、科学家的高度重视。由此可见, 网络战实施的广泛性必将使网络对抗成为新世纪的一种最突然、最难对付、破坏性最大的崭新作战形式, 成为军事实力和综合国力相对较弱的国家战胜强敌的法宝, "无硝烟 "的战争将重新演绎古典战争的内涵。

2　网络技术是网络战的关键

网络战是尖端高新领域的对抗活动, 是技术、知识密集型作战。网络战技术涉及到网络软件侦察与反侦察技术、网络软件攻击与反攻击技术、网络软件冒充与反冒充技术、网络软件控制权易位与反易位技术等。只有掌握了先进的网络技术, 才能进行网络侵入, 窃取情报; 修改、转移数据, 阻塞、改变信息流, 制造混乱; 截取指挥控制权, 误导敌人; 传播计算机病毒, 瘫痪系统节点; 预设 "逻辑炸弹", 伺机破坏等。由于网络对技术的过分依赖使得网络系统面对敌方的进攻而难以察觉。

2.1　网络攻击技术的运用

计算机网络攻击是进攻性信息作战类型之一, 是干扰、阻止、削弱或破坏敌计算机和计算机网络上的信息流或破坏敌计算机网络本身的作战行动。

(1) 获取口令。有三种方法, 一是通过网络监听非法得到用户口令, 这类方法有一定的局限性, 但危害性极大, 监听者往往能够获得其所在网段的所有用户帐号和口令, 对局域网安全威胁巨大; 二是在知道用户的帐号后利用一些专门软件强行破解用户口令, 这种方法不受网段限制, 但攻击方要有足够的耐心和时间; 三是在获得一个服务器上的用户口令文件(此文件成为 Shadow 文件) 后, 用暴力破解程序破解用户口令, 该方法的使用前提是获得口令的 Shadow 文件。此方法在所有方法中危害最大, 因为它不需要像第二种方法那样一遍又一遍地尝试登录服务器, 而是在本地将加密后的口令与 Shadow 文件中的口令相比较就能非常容易地破获用户密码, 尤其对那些口令安全系数极低的计算机网络, 可以在短短的一两分种内, 甚至几十秒内就可以将其破译。

(2) 放置特洛伊木马程序。特洛伊木马程序可以直接侵入用户的电脑并进行破坏, 它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载, 一旦打开了这些邮件的附件或者执行了这些程序之后, 它们就会注入正在使用的电脑中, 并在计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当使用者连接到因特网上时, 这个程序就会通知攻击方, 来报告所使用计算机系统的IP 地址以及预先设定的端口。攻击方在收到这些信息后, 再利用这个潜伏在其中的程序, 就可以任意地修改目标计算机的参数设定、复制文件、窥视整个硬盘中的内容等。

(3) 电子邮件攻击。电子邮件攻击主要表现为两种方式: 一是电子邮件轰炸和电子邮件 "滚雪球", 也就是通常所说的邮件炸弹, 指的是用伪造的 IP 地址和电子邮件地址向同一个信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件, 致使受害人邮箱被 "炸", 严重者可能会给电子邮件服务器操作系统带来危险, 甚至瘫痪; 二是电子邮件欺骗, 攻击者佯称自己为系统管理员(邮件地址和系统管理员完全相同), 给用户发送邮件要求用户修改口令(口令可能为指定字符串) 或在貌似正常的附件中加载病毒或其他木马程序, 这类欺骗只要用户提高警惕, 一般危害性不是太大。

(4) 通过一个节点来攻击其他节点。攻击方在突破一台主机后, 往往以此主机作为根据地, 攻击其他主机(隐蔽其入侵路径, 避免留下痕迹)。他们可以使用网络监听的方法, 尝试攻破同一网络内的其他主机; 或通过 IP 欺骗攻击其他主机。这类攻击很狡猾, 某些技术很难掌握(如 IP 欺骗), 是高技术攻击的有效途径。

(5) 网络监听。网络监听是主机的一种工作模式, 在这种模式下, 主机可以接受到本网段在同一条物理通道上传输的所有信息。此时, 如果两台主机进行通信的信息没有加密, 只要使用某些网络监听工具, 例如 NetXray 和 Sniffit, 就可以轻而易举地截取包括口令和帐号在内的信息资料。虽然网络监听获得的用户帐号和口令具有一定的局限性, 但监听者往往能够获得其所在网段的所有用户帐号及口令。

(6) 寻找系统漏洞。许多系统都有这样那样的安全漏洞, 其中某些是操作系统或应用软件本身具有的。这些漏洞在补丁未被开发出来之前一般很难防御攻击者的破坏, 除非将网线拔掉; 还有一些漏洞是由于系统管理员配置错误引起的, 如在网络文件系统中, 将目录和文件以可写的方式调出, 将未加 Shadow 的用户密码文件以明码方式存放在某一目录下, 这都会给攻击方带来可乘之机, 应及时加以修正。

(7) 利用帐号进行攻击。有的攻击方会利用操作系统提供的缺省帐户和密码进行攻击, 例如许多 UNIX 主机都有 FIP 和 Guest 等缺省帐户(其密码和帐户名同名), 有的甚至没有口令。攻击方用 Unix 操作系统提供的命令如 Finger 和 Ruser 等收集信息, 不断提高自己的攻击能力。这类攻击只要系统管理员提高警惕, 将系统提供的缺省帐户关掉或提醒无口令用户增加口令一般都能克服。

(8) 窃取特权。利用各种特洛伊木马程序、后门程序和自己编写的导致缓冲区溢出的程序进行攻击, 前者可使攻击方非法获得对用户机器的完全控制权, 后者可使攻击方获得超级用户的权限, 从而拥有对整个网络的绝对控制权。这种攻击手段, 一旦奏效, 危害性极大。

2.2 网络攻击战法的运用

(1) 使用特种部队进行作战。成立专门网络联合特种作战部队, 专职网络攻击和防护任务, 如美国空军 609 信息战中队, 美国防部"红色小组"等。此外, 特种部队装备计算机网络攻击设备将极大增强网络攻击的灵活性和可行性。同时利用专门的电脑病毒发射装置, 致使对方的飞机、导弹、坦克等带有电脑的武器装备系统因电脑程序错误而发生自我爆炸, 自我摧毁或相互残杀等, 从而影响战斗的进程。

(2) 遥控手段激活病毒。利用和平时期预先植入敌计算机网络系统中的病毒, 使用特殊无线电装置, 激活潜伏病毒, 即可实现对敌方计算机网络的破坏。

(3) 使用"灰色系统"作战。所谓"灰色系统"就是指介于交战双方的大量民用或第三国信息系统, 如民用电话设施, 国际互联网, 民用手提电话和无线电报等。利用"灰色系统"是一种途径, 也是一种手段, 因为在作战中无论哪一方, 都或多或少地使用这类系统。

网络攻击的威胁虽然很大, 但也不能一味地挖空心思去攻击对方网络系统, 同时要千方百计地寻找和利用保护自己网络系统的防御技术, 如电子盾牌、电子闸门、电子宪兵、自我修复等日新月异的计算机网络防御技术。

3 网络的安全防护

据资料显示, 每年世界各地的电脑黑客企图渗透到美国各军事专用网络的行为不少于 25 万次, 其中 65% 获得成功。而在每 150 次中只有一次被发现。在未来战争中, 对方只需掌握和破坏美国的军事专用网络, 即可严重削弱美国军用网络系统的能力, 进而取得战争的胜利。由此可见, 网络安全防护的重要性, 在注重网络建设的同时, 必须牢固树立网络安全的战略意识, 把网络安全摆在与网络建设同等重要的位置来抓。

对网络而言, 100% 的零风险就意味着网络的关闭, 但是在现有人力、财力和技术条件下, 以高度的安全意识、危机意识和全方位地解决网络安全问题, 则完全有可能把网络风险降低到最低限度。要认真做到这一点一是要牢固树立网络安全意识, 从战略高度认识网络安全的重要性, 做到"上网不泄密, 泄密不上网"; 二是要积极开展对网络安全问题的研究, 针对"病毒"入侵、"黑客"攻击、电磁辐射泄密做好防范工作; 三是要加强对军事信息系统建设的立项把关工作, 在考虑网络建设先进性、成熟性、开放性、适应性、灵活性等方面的同时, 更要加强网络建设的可靠性、安全性, 力争把网络的安全隐患消灭在立项阶段。

参考文献:

[1] 谢希仁. 计算机网络[M]. 大连: 大连理工大学出版社, 1999.

[2] 张 昕, 孙心义. 国内几种常见的上网方式[J]. 现代通信, 2000, (11): 33—36.

[3] 刘显林. 浅谈网络信息安全和保密问题[J]. 军网信息, 2001, (2): 21—22.