由科索沃危机中的网络战看中国未来的信息安全

郭永斌

摘 要 通过对此次科索沃危机中计算机网络战的剖析，可以看出网络战的安全内涵、所采用的手段及其利用的原理。从维护中国信息安全的角度出发，提出加强信息安全的 5 点建议：(1) 关键计算机软硬件必须走国产化道路；(2) 建立自己的计算机网络，一国两网；(3) 制订网络和系统的安全标准；(4) 建立和完善信息安全管理机制；(5) 加速信息安全技术与产品开发。

关键词 科索沃危机；网络战；信息安全
中图分类号 TP393.08 文献标识码 A 文章编号 1002-722X(1999)05-0109-03

近年来，信息革命的热浪席卷全球，全球互联网已遍及 100 多个国家和地区。网络的发展给整个世界带来了巨大的变化，同时也为各国带来了极为严峻的安全威胁。有关网络入侵、黑客攻击和计算机犯罪等基于网络的安全事件时有发生。在此次科索沃危机中，美国及其北约成员国盟友虽然占据了较大的空中优势，但其不义之举也招致了来自全球范围内计算机黑客的攻击。在这场无声的计算机网络战中，美国及其北约成员国并未占上风。

一、触目惊心的网络战

网络战是指以对手用于战争或者其它方面起重要作用的计算机网络系统为破坏和打击目标，通过各种手段窃取、窜改和破坏对方重要信息，使其计算机网络失灵、混乱和瘫痪，进而达到战胜对手的一种作战方式。在此次科索沃危机中，北约计算机系统频频遭到黑客攻击，损失惨重：(1) 3 月 29 日，俄罗斯电脑“黑客”入侵美国白宫网站，造成该网站无法工作。当天英国与西班牙的多处官方网站也遭到了破坏，北约国家轰炸行动中最依赖的英国气象局网站损失惨重；(2) 3 月 31 日，北约的互联网址及电子邮件系统受到南联盟黑客的侵袭，使其电子邮件服务器被阻塞；(3)“爸爸”、“梅利莎”、“疯牛”等病毒 4 月 4 日使北约的通信陷入瘫痪，美海军陆战队所有作战单元的 EMAIL 均被“梅利莎”病毒阻塞；(4) 北约在贝尔格莱德的 B92 无线电广播网服务器、北约布鲁塞尔总部的网络服务器和电子邮件服务器受到南联盟计算机黑客的攻击；(5) 北约网络负责人说，黑客还用“幸福 1999 宏病毒”攻击了北约的电子邮件系统，“幸福 1999 宏病毒”改变了微软公司应用程序的网络界面，并且发送一个可执行文件，这个文件令计算机屏幕显示焰火而崩溃；(6) 1999 年 5 月，北约暴行激怒中国黑客。1999 年 5 月 8 日，北约用导弹袭击我大使馆后，中国“民间黑客”纷纷对美国政府和民间的网站发起攻击。首先遭到袭击的是美国驻华大使馆网页（网址为：http//www.usembassy-china.org.cn）。该网页的中央被贴上了黄色大字——“打倒野蛮人”。9 日凌晨，美国白宫的网页遭到攻击，主页上两面美国国旗被换成了骷髅旗。随后，美国立法委员会的主页（http://www.capweb.net）成了黑客们的涂鸦板；10 日凌晨，美国能源部（http://www.apolo.osti.gov）被贴上了新华社与光明日报社遇难记者的照片。据统计，当时被中国民间黑客入侵的网站有：

http://www.whitehouse.gov 美国白宫站点
http://www.whitehouse.net 美国白宫站点
http://www.whitehouse.org 美国白宫站点
http://www.usembassy-china.org.cn 美国驻华大使馆中国服务器
http://www.capweb.net 美国立法委员会
http://192.41.140.35
http://199.211.115.79
http://www.iberlant.nato.int
http://www.ntao.org.tr
http://www.afsouth.nato.int
http://193.113.210.135
http://www.defenselink.mil
http://www.216.22.188.xxx XXX 为 0 到 380
http://nacced.org 美国国家经济发展与州经济发展联合会
http://mod.uk
http://www.nctsw.navy.mil 美国海军通信中心华盛顿站[1]

在这些站点中，级别最高、最有意义的被入侵网站是美国海军通信中心华盛顿站。但中国民间黑客的行为也遭到了国外黑客的报复，危机期间有新浪网、中文热讯、上海网盛（http://www.netsh.com）等网站也遭到了国外黑客的侵入。这些触目惊心的事件使我们不得不深深反思：我们的计算机网络安全吗？我们网络中是否存在着可被人入侵利用的安全漏洞？我们有没有可靠的安全审计措施？怎样才能防止自己的设备免遭攻击，保证自己的信息安全？

二、网络战的安全内涵

正如核技术在造福人类的同时也在威胁着人类的安全一样，计算机网络一方面给人类带来极大方便，另一方面也给国家的安

全带来了极大的挑战。在世纪之交审视因特网的安全内涵，对我国以积极的姿态应对未来世界政治的挑战，不无裨益。互联网对国家安全的挑战主要表现为以下 3 方面:

1. 政治文化的安全。对于非英语国家而言，已经面临着“殖民文化”的侵略。如今在互联网络上，英语内容约占 90%，法语占 5%，其他语系只占 5%。[2] 这样对相对落后的发展中国家而言，它们只能成为被迫接受信息的群体。发达国家通过网络向受众连续不断地传递文化信息，将其意识形态、价值观念强加于人，可以不战而胜般地影响受众对这些国家的感受和价值判断。受同一文化理念的长期影响，民众会对其产生亲近感、信任感，最后认同、依赖。与此同时对自己民族的自尊心、自豪感产生动摇。对此，美国哈佛大学肯尼迪政治学院院长约瑟夫·奈在 1996 年《外交》(三四月份合刊) 上登出的一篇文章可谓一语道破天机:“信息是国际领域的新型货币，美国在通过信息去扩展其‘硬型’和‘软型’的国力资源方面比其它任何国家都处于更有利的地位。”“作为一种国力资源的信息，其美妙之处还在于，它能在增加物质的军事国力的同时，不可抗拒地使社会民主化。希望维持中央权力而又能从信息中收获经济和军事实惠的共产主义和独裁政权，发现他们已经签署了一个浮士德式的协议。”

2. 经济的安全。经济力量是战争物资的主要依托。而据了解，到目前为止，我国银行、证券等国民经济要害部门的计算机网络的主机无一不是进口的。[3] 这样，如果网络黑客或某些别有用心者对通信、电力、金融、交通等关键性计算机网络进行有计划、有预谋的攻击，将严重威胁国家安全。据公安部门消息，1998 年全国破获黑客案件近百起，其中以经济为目的的网络犯罪占 61%。[4] 在国外也曾多次出现了利用网络对企业进行渗透的案件。如受雇于美国政府的一家安全服务公司发现，某国试图利用计算机系统改变美国一家钢铁制造厂生产的抗拉钢材的成分，目的是使钢材在冷冻状态下受到附加压力时发生断裂。[5]

3. 军事的安全。以计算机为核心的 C^4I 系统是现代战争中的中枢神经。在平时或战时将计算机病毒通过网络植入对手计算机的系统中，就足以破坏对方 C^4I 系统，使其指挥、控制功能处于一片混乱。有的计算机程序还可以窃取对方重要军事部门的情报资料，使其无密可保，处于被动。随着计算机网络技术的飞速发展，军队还面临着这样一个难题:在信息时代，战争不仅是民族与民族、国家与国家、阶级与阶级、政治集团与政治集团之间的最高斗争形式，也不仅仅表现为交战双方军队的对抗。国家可能不再是战争的唯一的发起者，企业、宗教团体、恐怖组织、部落游击队、贩毒集团甚至于个人只要拥有一台计算机和入网的电话线就可以对一个国家发起攻击。而且，由于这种攻击对防御一方来说预警时间极短，很可能在完全没有防备的情况下，就发生一幕“电子珍珠港”或“电子滑铁卢”的悲剧。

长期以来，我们十分重视捍卫领土、领空、领海的主权。如今面对无疆界的因特网，传统的国家主权观念必须重新审视。在信息社会，信息已成为国家利益的一个重要组成部分。“信息疆域”的大小、“信息边界”的安全关系到一个民族、一个国家在信息时代的兴衰存亡。可以肯定的说，因特网已成为继南极洲、外层空间之后又一轮国际竞争的新战略空间。

三、对网络发起攻击的方法和途径

计算机系统之所以容易遭到攻击，是因为其管理和应用上存在各种薄弱环节。美国国防部认为，目前攻击者侵入计算机系统的方法有投送邮件 (SENDMAIL)、口令破译和信息包嗅探等 3 种。

1. Sendmail。Sendmail 是 Internet 上使用的一种普遍的电子邮件类型。攻击者把居心不良的代码装入一份电子邮件中，并将其邮送到网络中某台计算机上。这种 Sendmail 不仅能够查明对方地址，而且能执行攻击者的命令。因为它是在系统的根层次实施的，所以能取得全部系统操作特权。

2. 口令破译。口令破译是指攻击者试图用猜测或窃取口令的方法来进入对方的计算机系统。目前这种方法已进入自动化，即攻击者无需自己去猜测合法用户的口令，而是由计算机来更为有效和系统地完成这种猜测。一般来说，由字母数字符号组成的复合口令比较难以破译，但即使在这种情况下，也可使用强力计算机来比较所有可能的符号组合，直到找到一种最佳匹配为止。

3. 信息包嗅探。信息包嗅探是在远地交换机或主计算机中偷偷地插入一种软件程序，用以监听网络中传送的信息包，并把所获取的信息副本发送给黑客的技术。据说，只要捕捉到一名用户的头 125 个按键动作，攻击者就能弄清口令和用户身分。

计算机网络侵入的方法如上所述，其利用的原理和漏洞有那些呢？只有认清这个问题，才能有效的进行信息防御。总的来说，安全问题可能产生于以下几个方面:

(1) 系统配置和管理方面的问题。我们目前采用的操作系统和一些应用支持软件都是通用的，这些系统的设计中有很多面向所有用户的缺省配置。当我们进行系统或软件安装的时候，可能并没有注意到这些缺省配置的存在。这样一些我们并不需要的功能就一直存在于系统中，而这些功能可能存在严重的安全漏洞。如有的用户系统中开放着匿名 FTP 服务，再加上对系统文件读写权限的不合理配置，使得任何人都能够通过这个服务获得一些重要的系统文件。又如有些用户的应用系统中有着层层安全措施，但系统的 ROOT 帐户却没有设置口令或仅设置了诸如“12345”之类的口令。

(2) 系统通信协议和应用服务协议中存在的一些漏洞。以 TCP/IP 通信协议为例，如果某用户在短时间内向服务器发送大量同步包，就能耗尽服务器所能容许的数量，使服务器无法接纳其它用户的正常请求。

(3) 系统或应用软件中的 BUG。BUG 是指程序中的一些问题和不足。寻找软件和系统的 BUG，利用它进行破坏是网络黑客们乐此不疲的工作，因而这些 BUG 也成了影响网络安全的一个重大问题。比如对 WINDOWS NT 可以发起这样的攻击:只要向 NT 服务器的特定端口发送特定的数据，就能破坏该 WINDOWS NT 系统。一般来说，软件厂商在得到某些 BUG 报告之后，会提供相应的补丁 (PATCH)。但一般的系统维护或网络维护人员往往不注意这些报告和补丁，使得系统的 BUG 迟迟没有得到更正，而威胁一直存在着。

(4) 进口软硬件中可能存在着安全后门。当今计算机上运行的系统软件几乎都是美国的产品，这些产品中很可能会保留一些安全后门，以便在必要的时侯打开这些后门进行破坏，特别是在发生国际政治、军事冲突的时候。

(5) 使用下载软件时可能带来的恶意代码。从 Internet 上可以下载到许多方便、实用的工具软件。有些 Java 程序也包含了可下载的可执行代码。这其中可能包含一些类似于“特洛伊木马”等危及系统安全的程序。

(6) 一些网络攻击的自动化工具。一些网络站点提供了用于网络入侵的工具，如扫描器、口令破译程序等。又如安全管理员分析网络工具 (SATAN)，它本来是为帮助网络管理员扫视他们的计算机以发现安全弱点而设计的，现在却成了一种有效的黑客工具。

四、如何维护中国信息安全

海湾战争后，美国拨出巨款用于计算机情报战的研究。在其“不对称作战”理论中，更是把防止对手利用计算机网络对其攻击放在了首要位置。对于像美国这样的信息军事大国，尚如此重视计算机情报战，其它国家无疑更应高度重视。应付计算机网络战的对策大致有以下几点:

1. 关键计算机软硬件必须走国产化道路。对于一个国家来说，从硬件设备到操作系统以及一些应用平台都采用进口设备是有危险的。如在刚刚发布的奔腾Ó CPU 芯片中就设置了用以识别用户身份的序列码。对此不少人指出，有了这种与机器永久相联系的序列码就相当于是在变相邀请别人窥视自己的机器。又如操作系统 WINDOW **98** 会根据用户的计算机硬件配置生成一长串与用户名字、地址相关的代码——全球唯一识别码，这个识别码会通过 WINDOW **98** 电子注册程序，在用户不知情的情况下将用户信息传送到微软的网站上去。从长远的观点来看，我们必须在重要的国家基础设施部门中使用自己的产品。这些部门除军事部门外，还要包括电信电力、天然气与石油储运、金融与财政、交通运输、供水、紧急求援 (医疗、警务、消防、救生等) 和施政管理部门等。研制完全独立属于自己的软硬件产品，以我们国家现在的技术水平来看显然还有较大的差距，但研制一些比较专用的设备和系统还是可能的。如我们现在已能依靠自己的能力生产大容量硬盘，而共享软件 LINUX 的出现为我们发展自己的操作系统提供了一次前所未有的良机。¼

2. 建立自己的计算机网络，一国两网。其根本目的是建立一个相对独立于因特网之外自成体系的国内互联网。该网络可将军队、各级政府机关、各企业单位、各事业单位及团体联结入网，形成一个庞大的融军事、行政、经济、科技、教育文化于一体的信息网络。这样即使我国国内的因特网被摧毁或中断，国内互联网仍可以正常运行。国内互联网应具有下列特征和功能: (**1**) 使用由中国人自己发明的软件系统，知识产权属于自己。(**2**) 技术构架符合现代潮流，采取将信息“推”出去的分散式树型结构。(**3**) 具有全中文界面；发布广告和查询信息简便。

3. 制订网络和系统的安全标准。实现网络安全应有一个安全标准，这个标准应对网络和系统安全的总体框架、各个方面的安全性以及它们之间的相互关联有一个严格的描述和定义。其中可以包括：管理制度方面的安全标准、系统和设备配置方面的安全标准、资源访问控制方面的安全标准、数据通信方面的安全标准、身份认证方面的安全标准、数据加密算法和密钥配置方面的安全标准、防电磁泄露方面的安全标准，等等。只有有了这样一些完整的标准之后，安全问题才有可能全面地解决好。

4. 建立和完善信息安全管理机制。如果一架轰炸机攻击一个国家的电厂，当然应由该国军队采取行动把那架轰炸机击落。但如果是**0** 与 **1** (计算机语言) 击毁了这个电厂，情况会怎样？这属于什么行为？应该由什么样机关对此做出响应？这是信息战超出军事范围的典型问题。对此一是要设置专门的政府机构来处理这样的问题。如 **1996** 年底，白宫内成立了所谓“总统关键基础设施委员会”，促成该机构成立的原因有两个: (**1**) 对有形财产的物理威胁。(**2**) 对控制关键基础设施的信息或计算机进行电子、射频或电脑攻击的威协。二是加强法制建设。如应制定有关防止和发现信息袭击并及时作出反应的政策，制定有关信息破坏、信息窃取和信息犯罪的法律法规。

5. 加速信息安全技术与产品开发。当代信息防御技术包括多级安全、标准信息卡、密钥管理和加密体制等。具体的安全产品如: (**1**) 防火墙产品。它主要提供被保护网络与外部网络之间的进出控制。(**2**) 安全路由器。安全路由器提供了某些基于地址或服务的过滤机制，可以在一定程度上限制网络访问。(**3**) 安全监测预警系统。主要用于监视网络上的数据流，寻找具有网络攻击特征和违反网络安全策略的数据流，当发现可疑数据流时即按照系统安全策略进行相应反应。反应包括实时报警、记录有关信息、实时阻断非法的网络连接、对事件涉及的主机实施进一步的跟踪等。(**4**) 身份认证系统。身份认证系统加强了原有的基于帐户和口令的访问控制。目前的身份认证系统有一次一密的认证机制，有基于时钟的动态口令机制，有基于生理特征的认证机制等等。(**5**) 信息网关。信息网关负责检查出入网络的文件是否具有网关证，是否按照所具有的密级要求进行了加密，在检查合格后文件才能传出网络。(**6**) 安全性分析工具。安全性分析工具用于自动发现网络上的安全漏洞，给出安全分析报告，作为重新进行网络安全配置的依据。

注　释

¹ 见《电脑报》**1999** 年 **5** 月 **17** 日，这一资料得到《解放军报》**1999** 年 **7** 月 **27** 日第六版《重视研究网络作战》一文证实。

º 《光明日报》，**1999** 年 **5** 月 **26** 日。

» 《人民日报》，**1999** 年 **8** 月 **9** 日第十二版。

¼ 《中国青年报》，**1999** 年 **3** 月 **1** 日。

½ (美)《基督教科学箴言报》，**6** 月 **24** 日。

¾ **1999** 年 **5** 月 **21** 日，长城集团在北京推出了第一块中国自主生产的 **8**. **6**GB 的高容量高速硬盘。见《光明日报》**1999** 年 **5** 月 **26** 日。

参考文献

[**1**] 电脑报. **1998** 年合订本；**1999** 年 **5** 月 **17** 日.

[**2**] 阿尔文·托夫勒著. 未来的战争. 新华出版社，**1996**.

[**3**] 现代军事. **1998** (**10**).

[**4**] 李际均著. 军事理论与战争实践. 军事科学出版社，**1994**.

(作者单位：解放军外国语学院二系　**471003**)

(责任编辑　赵德远)