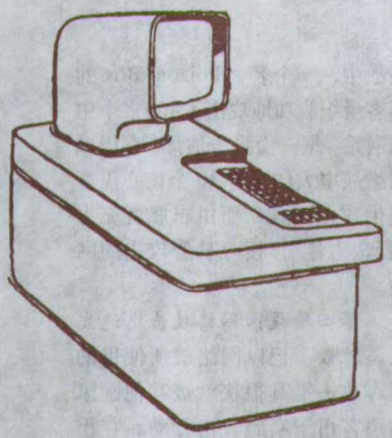


# 未来网络战——什么样

●[美]帕特里克·艾伦 克里斯·德姆查克
○张宏飞 钟 实 编译

2000年9月，以色列的一群年轻黑客创建了一个网站，以拒止服务的方式持续发动网络攻击，成功地瘫痪了黎巴嫩真主党游击队、哈马斯组织以及巴勒斯坦国家安全部的6个网站。这次网络攻击引发了一场迅速升级的国际网络战。巴勒斯坦人及伊斯兰组织呼吁发动一场网络“圣战”。不久，伊斯兰黑客攻击了分属于以色列政府、外交部和国防部的3个网站，随后还攻击了以色列总理办公室、以色列银行和特拉维夫证券交易所的网站。

巴以网络战虽然未使相关国家造成严重的物质损失，但这次网络冲突的一些因素却非常重要，因为它们将成为未来网络战的模式。2001年5月，由撞机事件引发的中美网络战与巴以网络战具有相似的特征。

## 巴以网络战始末

巴以黑客间的冲突始于1999年，在2000年9月底骤然升级。至2001年1月底，冲突双方攻击了160个以方网站和35个巴方网站，其中包括至少一个美国网站。从1999年7月至2002年4月，548个以色列网站主页遭损，同期有1295个中东地区网站主页遭损，还有一些以方网站受到了严重的拒止服务攻击。

网站页面损毁和分散式拒止服务是黑客采用的两种主要攻击方式。前者主要针对高层政治类网站（如政府网站）。在某些情况下，网上贸易交易量也会因为主页遭损而有所减少。一方黑客发动攻击所使用的服务器通常也会被另一方黑客用于发动类似攻击。一方编写的用于攻击对方网站的代码也会被对方重写后进行反击，后者则迫使对方网站关闭数日，并使该地区互联网基础设施的网络信息量急剧增大。

黑客的攻击目标还包括美国电报电话公司等电信基础设施公司。据说该公司曾协助以色列扩大被攻击网站的带宽。一名叫多迪的亲巴勒斯坦黑客损坏了一家为以色列政要提供服务的网络服务供应商的主页，并留下信息声称，他可以关闭以色列Net Vision网络服务供应商的服务器。该供应商拥有以色列70%的互联网资源。

2001年11月8日，一个名为“团结”的极端组织宣称，它已开始实施4阶段战略的第三个阶段的行动。第一个阶段主要是破坏以色列政府的官方网站。第二个阶段包括对以色列银行和特拉维夫证券交易所实施攻击。第三个阶段的攻击目标包括以色列网络服务供应商基础设施及朗讯和“金线”公司（以色列电信服务供应商）的网站。该组织宣称将延期实施第四个阶段的行动，即破坏以色列的电子商务网站，并对大额网上交易构成威胁。

以色列的“互联网地下组织”由一群帮助以色列提高网络安全水平的黑客组成。它声称已出现第四个阶段攻击的迹象。这些攻击包括破坏一些具有电子商务功能的工商类网站。“互联网地下组织”确信这些攻击使以色列证券交易所的交易额下降了8%。

虽然过去数年间中美黑客仅进行过零星的网络战，但2001年的中美撞机事件却引发了大规模网络战。中国黑客增加了针对美国的行动，并试图在2001年5月的第一周组织大规模黑客攻击行动。与此同时，美国黑客对中国扣留EP－3侦察机乘员的做法表示愤怒，并开始组织实施“中国杀手”行动。

## 巴以网络战对我们的启示

基于对巴以和中美网络战的观察，可确信未来的网络战将分为4个阶段。

*第一阶段：交战和应战。*巴以网络战清楚地揭示了进行网络袭击的方式。以方黑客起初采用页面损毁和拒止服务的方式对巴方网站发动突袭。当巴方宣称向以方发起网络“圣战”时，其黑客也针对以方网站取得了同样的突袭效果。以色列人对本国公民首先挑起网络战以及巴方反应和本国政府与民间网站的脆弱程度感到震惊。之后，双方都用一段时间修复系统损伤，以加强应对未来攻击的防护。

网络战最初的攻击效应是一个值得研究的问题。Jerusalembooks.com是以色列最大的网上书店网站。由于网站页面受损它被迫关闭数日。该公司面临着数日的销售额损失以及消费者对网络交易安全性的担忧。同样，以色列国土管理部的网站也被迫关闭数月。对于以色列

而言，网站被迫关闭的情况使国民信心受挫。此外，大量的页面损毁和拒止服务攻击（2000年10月6日至12月2日期间在该地区共发生了115次）使中东地区互联网基础设施不足的现状更趋恶化。

据名为“现实研究”的机构评估，2002年世界范围内因网络攻击造成的损失超过了1.5万亿美元。

*第二阶段：冲突迅速升级。*巴以网络战开始后的4周内，巴方黑客就攻击了美国网站。3周后，以方黑客攻击了伊朗和黎巴嫩的网站。由于以方发起反攻的网站数量比巴方更多，因此以方黑客开始寻找巴勒斯坦国家安全部和黎巴嫩网站之外的防护较为薄弱的目标。例如，自称“摩萨德”的以方黑客就损坏了伊朗总统的网站，并声称伊朗是黎巴嫩恐怖组织的支持者。

网络战比常规战争具有升级更快的特性，原因有3个。第一，民间黑客选择攻击目标的首要标准是易攻击性，而不是重要性。在搜寻到某个易遭攻击的目标之前，其搜寻范围一直在不断扩展。如果目标国的政府和商业网站不易攻击，那么与该国友好国家的网站将会遭到破坏。反之，受雇于特定国家的职业黑客只有在对目标国形成预期攻击效果的情况下，才有可能使攻击升级。第二，国际黑客组织将当前形势视为它们可以在不受报复的情况下发动攻击的良机。许多黑客都想显示他们的能力，而网络具有大众传播功能。因此对网上任何目标的攻击都会使其名声远扬。第三，迄今为止，网络战都呈现出两极分化的特征。一场网络冲突（如巴以网络战）两极分化的特征越明显，双方吸引支持者的机率就越大。双方都认为对方拥有坚定的支持者，因此在巴以网络战开始后不久，美国就被视为与以色列相同的被攻击目标。

在传统意义上，交战国双方的盟国若不直接参战，相对都比较安全。那些试图将冲突升级的国家在采取将中立国拖入战争的做法时，其代价将是遭到相应的惩罚。然而在网络空间，对于某国而言，促使冲突升级的代价很小，对于单个的黑客而言则基本上不存在代价。因此，未来的网络冲突将呈现快速升级的特征。

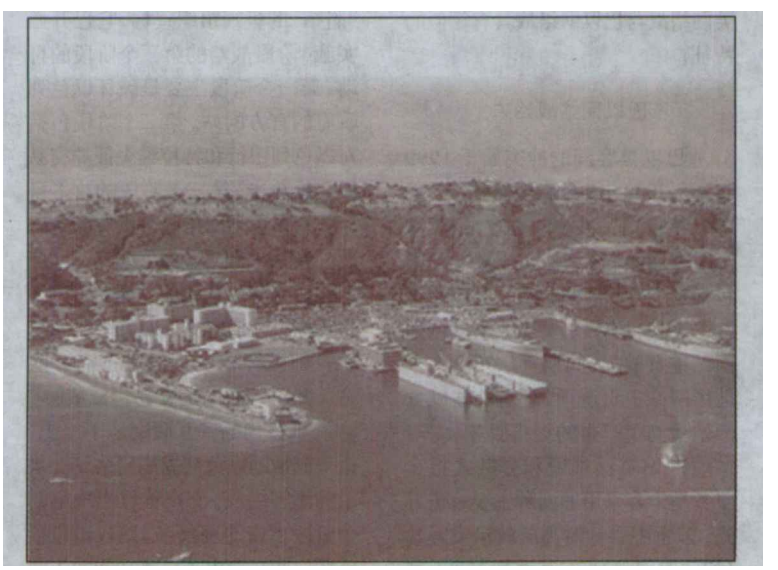
*第三阶段：冲突迅速国际化。*网络战将吸引两类人员。一类是经常参与国际网络冲突的优秀黑客群体，第二类是满怀爱国激情的业余黑客。巴以网络战吸引了来自以色列、巴勒斯坦、黎巴嫩、沙特阿拉伯、巴基斯坦、巴西及美国的黑客。向以色列发起的网络攻击绝大部分都源自于以色列或巴勒斯坦国家安全部门之外。值得注意的是，多个巴西黑客组织在巴以网络战中向巴以双方发动了攻击。它们很显然是想在网络战的双方参与者面前显示其攻击技能。在中美网络战中，来自美国、沙特阿拉伯、巴基斯坦、印度、巴西、阿根廷和马来西亚等国的黑客站在美国一方，而来自中国、日本、印度尼西亚和韩国的黑客则站在中国一方。值得注意的是，除非在那些互联网受到政府严格控制的国家，否则黑客间的联盟并不一定反映国家的意愿。

一个或一群黑客有能力在较短时间内造成大量破坏。在中美网络战中，一个名为Poizon Box的黑客组织成功地攻击了400多个中国网站。据一份报告估计，在巴以网络战中大约只有30个核心黑客提供攻击工具，而由志愿者充当“野蛮力量”，搜寻易遭攻击的网站。

*第四阶段：网络攻击迅速发展与扩散。*巴以网络战所使用的黑客攻击工具很快就被其他国家的黑客用于实施攻击行动。在巴以网络战中，以方黑客研制了一种新型网页损毁和拒止服务攻击工具。美国的一些年轻黑客从以色列黑客手中获得了这种攻击工具，并计划在2001年元旦利用这种工具发动一次全球性网络攻击。幸亏美国联邦调查局察觉到了这一密谋，否则这次攻击将会在当天对互联网造成严重破坏。

在网络战中，黑客们使用了一种名为carko的工具。这种工具不仅试图破坏目标系统，而且还使用缓冲区溢出的攻击方式输入新的根密码，或在目标系统从攻击中恢复过来时在该系统安装一个后门，这意味着被carko攻击过的系统有可能遭到后续渗透。

虽然损毁网页和拒止服务攻击方式此前已为外界所知，并在



今年初，一名18岁西班牙青年打入美国圣迭戈海军基地绝密电脑安全系统，严重干扰了美军基地的正常活动。网络战主体已经悄无声息地发生了变化。

上述攻击前被使用过，但在未来只拥有有限带宽的单个黑客也可能具备实施大规模损毁网页和拒止报务的攻击能力。这种攻击可通过一个传输速率为56K的调制解调器和一个非对称数字用户线路（ADSL）实施攻击，并可通过网络服务传播器放大1万倍，从而使攻击规模达到一条T1传输线路的2/3。本·文兹克指出："通过此类攻击工具，一个56K的调制解调器将会变成一种威胁强大的武器，而带宽则成为无关紧要的东西。"因此，几个通过调制解调器联结在一起的便携式笔记本电脑就能够发动规模相当于几条T1线路甚至T3线路的网络攻击。这类攻击将使绝大多数系统陷入瘫痪。

除通过传播网站发动网络攻击外，黑客们还使用另一种途径实施攻击，即将软件置于其他服务器中并在某一特定时间启动该软件。这些被感染的服务器被称为"还魂尸"，即它们毫无"知觉"地参与到了网络攻击之中。美国联邦调查局发现，在一次范围较广的网络攻击中，220个互联网网址的560台服务器被感染。

**总之，网络攻击的发展速度呈现出不断增加的趋势，这与战时武器研制速度加快的趋势相似。然而更具挑战性的是，网络战的扩散速度比传统战争的扩散速度要快得多。**

**国际社会如何应对？**

在任何一次现代冲突中，网络都将成为另一种攻击路径。而且每一次网络冲突都会促进网络攻击手段的发展，并使其迅速散布至全球范围内的黑客。这种扩散对于监视网络战中黑客攻击工具的使用以及新网络技术的发展具有重要启示。除监视这些新工具的破坏能力之外，各国还有必要监视那些无法抵御运用这些新工具诱惑力的业余黑客的网上交流。因此，每个国家都有必要研究制定应对措施，以阻止新式网络武器的使用或削弱其攻击效果，有必要定期对服务器进行扫描以搜索潜伏式攻击软件，以此缩小其在未来发起攻击的范围。各国通过了解和掌握新的黑客攻击工具和方法，将能对这种攻击进行有效预防或降低其攻击效果。

（刘忠顺摘自《世界安全》）

# 丰 碑

●李本深

一支长长的红军队伍在云中山的冰天雪地里，顶着混沌迷蒙的飞雪前进。严寒把云中山冻成了一个大冰坨。狂风像狼似的嗥叫着，要征服这支装备很差的队伍。

将军的马早已让给伤号骑。将军和战士们一道踏着冰雪行军。他不时被寒风呛得咳嗽着。他要率领这支队伍向前挺进，为后续部队开辟一条通道。等待他们的将是十分恶劣的环境和十分残酷的战斗，可能三天两头吃不上饭，可能要睡雪窝，可能一天要走一百几十里路，可能……哦，可能太多了，这支队伍的素质怎么样呢？能不能经受住严峻的考验？

将军思索着……

前面的队伍忽然放慢了行军的速度，有许多人围在一起，不知干什么。

将军边走边喊：不要停下来，快速前进！

将军的警卫员回来告诉他："……前面……冻死了一个人……"

将军愣了愣，什么话也没说，朝那边走去。风雪太大了。他步履有些踉跄，眼睛有点迷离。

一个冻僵的老战士倚靠一棵光秃秃的树干坐着，一动也不动，好似一尊塑像。他浑身都落满了雪，可以看出镇定、自然的神情，却一时无法辨认面目，半截待卷的旱烟还夹在右手的中指和食指间，烟火已被风雪打熄。他微微向前伸出手来，好像要向战友借火……"怎么？他的衣服这么单薄、破旧？像树叶，像箔片一样薄薄地贴在身上……他的御寒衣物呢？为什么没有发下来？"

将军的脸上顿时阴云密布，嘴角边的肌肉明显地抽动了一下，蓦然转过头向身边的人吼道："叫军需处长来，老子要……"一阵风雪吞没了他的话。他红着眼睛，像一头发怒的豹子，样子十分可怕。

没有人回答他，也没有人走开……

"听见没有？警卫员！快叫军需处长跑步上来！"将军两腮的肌肉大幅度地抖动着，不知是由于冷，还是由于愤怒。

终于，有什么人对将军小声地说了一声："这就是军需处长……"

将军就要发火的手势突然停住了。他怔怔地伫立了足有一分钟。雪花无声地落在他的脸上，融化成闪烁的泪珠……他深深地呼出了一口气，缓缓地举起了右手，举至齐眉处，向那位与云中山化为一体的牺牲者敬了一个庄严的军礼……

雪更大了，风更狂了。大雪很快覆盖了军需处长的身体。他变成了一座晶莹的丰碑……

将军什么话也没说，大步地钻进了弥天的风雪之中。他听见无数沉重而又坚定的脚步声在说："如果胜利不属于这样的队伍，还会属于谁呢？"

（黄家祥摘自2006年4月27日《现代知音》）