浅议网络战中的国际法问题

□ 田 英

（南京政治学院　江苏·南京　210003）

摘　要　网络战作为现代高技术战争的重要作战样式，在上世纪末本世纪初的几次战争中已崭露头角，并在战争权、作战的手段和方法、人道主义保护、战时的中立及战争的犯罪和惩处等方面都对现行国际法提出了挑战。我国在坚决遵守国际法规条约的基础上，要积极参与适用于网络战的国际法条款的制定，并要严厉谴责别国违反国际法基本原则的网络攻击行为。

关键词　网络战　国际法　战争法

中图分类号：D99　　文献标识号：A　　文章编号：1009-0592（2007）-198-02

1991年海湾战争开战前，美国中央情报局知悉伊拉克从别国采购了用于防空系统的打印机，便派特工将病毒芯片植入打印机并运抵伊拉克。美军在空袭之前以遥控手段激活了病毒，使其从打印机窜入主机，致使伊拉克防空指挥中心主计算机程序和军队自动化指挥系统均发生错误，无法正常工作，为美军实施空袭铺平了道路。①

1999年的科索沃战争中，北约组织了为数不少的计算机专家将大量的病毒和欺骗信息输入南联盟军用计算机互联网络和通信网络，以阻塞其信息传播渠道。南联盟也没有示弱，众多黑客的集团作战致使美国白宫的网络服务器曾一度无法工作，另外，“梅莉沙”、“疯牛”等病毒的注入造成了北约军队计算机信息通信系统的局部瘫痪。②

2003年3月，伊拉克战争正式打响，但另一个空间的战火早在一个月前就燃起了。2月底的短短几天内，数千名伊拉克人在他们的电子邮箱里看到一封发信人被掩盖的邮件，“放弃吧，起义并倒戈，到另一边来，否则美国就开战了。”在战争进行过程中，美军的‘网络特种部队’使用2000多种计算机病毒对伊拉克的军事通信系统进行了摧毁性的攻击，致使伊拉克军队接受错误信息或得不到任何信息。

三次战争共同说明了一个问题：网络战作为现代高技术战争的重要作战样式，已经正式登上了历史的舞台。

一、网络战的提出

进入90年代以来，计算机技术的发展与应用在网络方面取得了极大的突破，形形色色的局域网和互联网风起云涌，迅速覆盖到世界的各个领域，其中也包括军事领域。计算机和网络技术的发展也促进了战争形态的演变和发展，“网络战”这个新名词开始频繁地出现在我们的视野中。

网络战是为破坏敌方信息网络系统的使用效能和保障己方信息网络系统正常发挥效能而采取的综合性行动。网络战有广义和狭义之分。广义的网络战是指敌对双方在政治、经济、科技和军事领域运用网络技术，为争夺信息优势而进行的斗争。狭义的网络战是指敌对双方在军事领域，主要包括作战指挥、武器控制、战斗保障、后勤支援、军事训练、情报侦察、作战管理等方面，运用网络技术所进行的一系列网络侦察、网络进攻、网络防御和网络支援行动。③广义的网络战早已发生，而狭义的网络战即军事意义上的网络战才刚刚拉开帷幕。

二、新兴网络战对现行国际法的挑战

国际法主要是调整国家之间关系的法律体系（包括原则、规则和规章制度的总体），④不仅调整平时国家之间的关系，更重要的是调整战时国家之间的关系。国际法中的战争法对战争的开始和结束、作战的手段和方法、人道主义保护、战时的中立及战争的犯罪和惩处都做出了明确的规定和限制。任何形式的战争都要严格服从于国际法和战争法的制约，但问题在于，国际法的制定严重滞后于现代战争的发展。网络战作为一种基于互联网的全新的作战形式，国际法中还没有明确的规则来规定和制约它，所以网络战的作战行动使现行国际法面临着严峻的挑战，主要体现在以下方面：

（一）颠覆传统的领土及主权概念

“互相尊重主权和领土完整”是国际法最基本的原则之一。拥有主权和领土完整是一个国家之所以成为国家的主要标志。主权是指一个国家独立自主地处理内外事物的权力，而领土是指处于国家主权支配和管辖下的地球的特定部分。对一个国家的主权和领土的任何形式的侵犯都是严重违反国际法的。而网络却恰恰是无国界的，互联网几乎遍布世界的各个角落，在网络世界中很难精确界定各个国家的主权和领土范围，所以在网络战中很难判定哪个范围哪个程度的网络攻击属于“侵略”的范畴，因此国际社会也无法用相关的国际法规则来制裁实施网络攻击的国家。

（二）较难追究国际损害行为的责任

国际损害行为是指某一国际法主体从事的、给其他国际法主体造成损害性后果的、国际法允许或不加禁止的行为。⑤国际损害行为的主体可以是国家，也可以是经国家或政府正式授权代替国家行事的个人和团体。做出国际损害行为的国家是要负赔偿责任的。在以计算机为武器的网络战中，精通计算机和网络技术的电脑黑客数不胜数，他们只要拥有电脑和入网线路就可以随时随地对任何一国的网络系统进行攻击，而且不需要经

过国家授权。黑客的网络攻击行为造成他国损害，可被攻击国却很难准确地知道攻击者到底是敌国严密组织的“网军”还是自发的黑客所为，自然就较难根据国际法追究国际损害行为的赔偿责任。

（三）合法自卫原则难以适用

国际法规定，自卫是各国都享有的自然权利，是遇到武力攻击时或是针对迫在眉睫的进攻。[6]在网络战中，网络攻击行为往往是相互交织的，难以判断是哪一方先发起了攻击，况且这种虚拟世界中的攻击行动能否被定义为“武力攻击”或“迫在眉睫的进攻”还是一个未知数。受到网络攻击的国家能否以同样的网络武器自卫还击也没有在国际法中明确规定，可以说为网络黑客们留下了法律空白。

（四）宣战原则难以适用

“开战前必须宣战”是国际法的规则。但目前国际社会还没有形成统一的说法将网络空间的对抗行动归入正式的“战争”，“网络战”只是一个提法，并未正式写入国际法中。况且，在网络攻击中，不管是政府组织的“网军”还是自发行动的黑客，很少有“先宣再战”的，攻击前宣示的做法会大大降低网络袭击的作战效能，因此国际法中的宣战原则在网络战中难以适用。

（五）对区分原则的挑战

区分原则是战争法中作战方法的首要原则。即任何作战首先要区分军事目标与非军事目标、区分平民与武装部队、区分战斗员与非战斗员、民用物体与军用设施，禁止不分皂白的攻击。网络战原则上只应针对军用网络，但由于网络的开放性，军用网络不可能与民用网络完全隔离，在某些领域某些时刻军用网络甚至是与民用网络高度互联的。在这种情况下，对军用网络的攻击是不可能不波及民用网络的，甚至一些关系国计民生的政府及重要部门网络系统也会受到影响而无法正常运作，给被攻击国造成难以估计的经济损失。另外，网络战的作战力量已趋于大众化，不管是军人还是平民，只要精通信息及网络技术，就可以发动网络攻击，所以说网络战是“全民皆兵”，难以辨认战斗员与非战斗员。

（六）对军事必要原则的挑战

军事必要原则强调采取任何作战手段和作战方法必须从是否有必要出发。绝大多数网络战都是辅助兵力火力作战的，很难说哪种网络攻击是绝对必要的。

（七）难以界定网络欺骗的合法性

背信弃义与诈术都是出于对敌方欺骗的目的达到作战效果，区别在于前者是非法的，而后者是合法的。国际法对二者的区别作了详细的阐明。网络欺骗是指在计算机网络系统中所实施的信息欺骗，网络宣传欺骗、虚拟现实欺骗、“黑客”欺骗和病毒欺骗等是其常用方式。[7]由于网络欺骗技术的多样性，很难判断它是属于诈术还是背信弃义，因此难以界定它的合法性。

（八）无从保护中立国的利益

由于网络攻击的形式丰富多样，所以查证和确定攻击源就十分困难。网络遍布全球，中立国的网络系统和资源很有可能被交战一方的“网军”或黑客利用来攻击敌方的作战通信和指挥网络，而中立国政府却不曾觉察，即使觉察了也难以查证攻击源及攻击者，保护中立国的利益无从谈起。

（九）对战争犯罪的惩处难以实施

如上所述，网络战的攻击源和攻击者难以查证，那么对攻击者的惩处也就变成了一纸空谈。

三、网络战中的国际法应对

（一）遵守现有的国际法规条约，避免自己陷入被动

国际法有一条基本原则：条约必须遵守。我国除了对少数危害我国主权的国际法公约和条款予以抵制和保留外，已经批准加入了大多数国际法战争法公约。我国要严格恪守已加入的国际法规条约，避免自己在未来战争中陷入被动。现代网络战中对国际法规的遵守主要体现在以下几个方面：

1.对战争权的运用

根据国际法规定，只有几种特殊情况才可以使用武力。[8]应用到现代战争，我方应坚持绝不在非特殊情况下首先发动网络攻击。

2.遵守“军事必要”原则，严格区分打击目标

在未来的网络战中要严格区分军用网络和民用网络，民用网络属于受国际法保护、免遭攻击的民用设施，对民用网络进行任何形式的攻击和破坏，都属于违法行为，要受到相关国际法的制裁。

3.不肆意扩大战争范围，保护中立国

在网络战中应谨选作战目标，绝不主动攻击中立国的国家网络，也绝不利用中立国的国家网络去攻击敌方。

（二）积极参与制订适用于网络战的国际法规或条约

国际法及战争法的制订严重滞后于现代战争的发展，尤其是网络战，针对网络战的立法问题迫在眉睫。由于少数大国掌握了互联网的核心技术，他们极有可能以此为借口操纵国际社会针对网络战的立法权，为自己掌控未来战场谋得便利。迫于这种形势，在互联网技术上不占优势的国家便要联合起来，积极参与制订适用于网络战的国际法规或条约，对网络战作出严格的规范，维护自己的合法权益，有效遏止少数大国的网络霸权，努力争取网络世界的和平。

（三）严厉谴责敌方违反国际法基本原则的网络攻击行为，争取国际社会舆论支持

当我方受到网络攻击时，不应首先选择报复，因为报复与反报复只会让战争无限升级。我方应将敌方的网络攻击行为上诉到联合国，严厉谴责敌方违反国际法基本原则的网络攻击行为，争取国际社会舆论支持，通过国际社会和平解决网络争端。

（四）培养自己的“网军”，为组织有规模的网络战做准备，在不违反国际法原则的基础上发动网络攻击，达到己方作战目的

为适应未来的网络战争形势，我军也应成立一支担当特殊使命的网络特种部队，使它成为我方的“网军”，有规模地组织网络进攻与网络防御，捍卫我军的信息安全，加强信息基础设施的建设和信息网络技术的发展，在不违反国际法基本原则的基础上在网络空间与敌展开对抗，达到我方作战目的。

注释：

①②马亚西，成冀，王汉水.网络战.国防大学出版社.1999年版.第66，69页.

③李耐国.信息战新论.军事科学出版社.2004年版.第80-81页.

④⑤卢纪元，来云龙，成盛昌.国际法.海潮出版社.2000年版.第1，73页.

⑥⑧丛文胜.战争法原理与实用.军事科学出版社.2003年版.第188页.

⑦于巧华，周碧松.网络信息战.解放军出版社2001年版.第162页.