网络战的国际法应对

刘　正
(南京财经大学法学院, 江苏 南京　210003)

[摘要]　网络战(又称信息战)的始作俑者美国正积极准备网络战, 世界其他国家积极跟进。网络战危害巨大, 其"颠覆"了现行战争法。补充和完善现行战争法以应对网络战成为当代维护国际和平、安全的重大的紧迫课题。

[关键词]　美国;　网络战;　现行战争法;　补充和完善
[中图分类号] DF938　[文献标识码] A　[文章编号] 1003—4145[2006]03—0139—03

在 1991 年的海湾战争前, 美国事先将一套带有计算机病毒的芯片换装到伊拉克购置的用于防空系统的打印机中, 美军空袭伊拉克后, 用无线遥控装置激活潜伏的病毒, 致使其防空系统瘫痪。1999 年的科索沃战争中, 美国黑客潜入南联盟空军的计算机网络系统, 使南军把大量的假目标当成了北约的真飞机。而南联盟黑客运用"梅莉莎"病毒攻击美国海军陆战队, 造成"尼米兹"号航母的计算机系统瘫痪 3 个多小时。这样人类发明的造福于人类的计算机互联网这个虚拟空间也出现了战争——网络战。

一、网络战的登场与危害

网络战(又称信息战)的始作俑者美国正积极准备网络战, 具体包括: 1. 组建信息战指挥机构。2. 组建信息战作战实体。3. 研制信息战武器系统。4. 建设数字化战场。[1](P289-290)美军方透露, 数项绝密黑客计划正在进行中, 有关网络战的全新战争政策和交战规则也在制定中。世界其他国家积极跟进。1. 俄军将网络战称为"第六代战争", 强调在网络战中"先机制敌", 实施主动性的信息攻击措施。俄国技术专家正在加紧开发研制用以破坏或降低敌电子信息系统效能的计算机病毒武器。2. 英军组建网络作战单位, 在计算机业界招募相应的信息技术专家。3. 日本防卫厅根据其 2005- 2009 年《中期防卫力量发展计划》, 正在组建一支由陆海空自卫队参加、人数多达 5000 人的网络部队, 专门负责执行反黑客、反病毒入侵任务。4. 法国、德国也在加强网络作战的研究与发展建设, 已基本形成了自己的网络战理论, 相继成立了网络战机构或部队, 并公开招募相应的信息技术专家。5. 印军同印度科学院、印度技术学院等专业机构进行技术合作, 提高网络战能力, 组建了陆海空三军联合计算机应急反应分队, 招募黑客入伍, 已开通使用代号为"闪光信使"的战略宽带卫星网。6. 据韩国媒体报道, 朝鲜的"黑客"部队约有 500 人, 已具备对美国、日本、韩国发动网络作战的能力。其实, 韩国国防部从 2000 年始, 将国防预算增加了 5%, 专门用于提高应对网络战的核心技术。

通常来说, 网络战分为广义和狭义两类: 广义网络战指全球战略网络战, 是指国家或集团围绕和运用计算机网络进行的政治、经济、文化、科技和军事等斗争; 狭义网络战是战场网络战, 是指交战双方围绕和运用战场互联网进行的对抗。

从网络战攻击模式来看, 主要有: 体系破坏模式, 通过发送计算机病毒、逻辑炸弹等方法破坏敌计算机与计算机网络系统, 以造成敌国指挥控制系统瘫痪; 信息误导模式, 向敌计算机与计算机网络系统传输假情报, 改变敌计算机网络系统功能, 可对敌决策与指挥产生信息误导; 综合模式, 综合利用体系破坏和信息误导, 并与其他网络战模式结合, 造成对敌多重杀伤功效。

随着各国对网络战研究的深入, 网络战所发挥

收稿日期: 2005- 09- 01
作者简介: 刘　正(1965-), 江苏镇江人, 南京财经大学法学院副教授, 研究方向: 国际法学。

的作用已与核武器等同甚至超过核武器。像美国重要智库兰德公司提出了“战略战”的概念，认为战略战是一种破坏性极大的“顶级”作战形式，它实施的成败关系到国家的安危与存亡。兰德公司指出，工业时代的战略战是核战争，信息时代的战略战主要是网络战。

军事专家指出，网络战与核战争比，既存在相同之处，又有区别。同核战一样，网络战产生的破坏力巨大。网络战一旦全面展开，遭受攻击并被击败的一方有可能遭受国民经济全面崩溃的危险。核武器通常可以产生巨大的心理震憾效果，网络战同样可崩溃敌人的战斗精神和意志。核武器一旦使用后，战争后果具有不可控性，网络战也是如此，像病毒之类的作战武器在释放之后，将无法控制，可能具有“双刃剑”效应。而网络战与核战最大的不同在于网络战的胜利不是以大量的生命为代价，战争的附带毁伤小。[2]

据美国国防部估计，已有 120 个国家具有计算机攻击的能力。西方学者认为信息武器具有对政治、经济、文化、科技、外交、军事、社会和意识形态等极强的穿透力和攻击力，最具危险的破坏力，对之难以做到真正的全面防范。当前一场争夺“制网权”、“制信息权”的新一轮军备竞赛已在全球展开。笔者认为随着计算机互联网科技一日千里的发展，放任不管，网络战的作战能力、危害将越来越大。[3](164)

二、网络战对现行战争法的“颠覆”

现行国际法既调整和平时期国家之间的关系，也调整战争时期国家之间的关系。现行战争法（又称武装冲突法）以国际条约和国际习惯法的形式规定了一系列原则、规则和制度，具体包括：战争开始、结束及其法律后果，作战手段、作战方法的限制，对战俘、平民、民用物体、文化财产的人道主义保护，陆战、海战、空战法规则，中立规则，战争犯罪及惩处。

信息战的出现对现行武装冲突法提出严峻的挑战，造成了巨大的冲击。有学者提出了下列问题：“一个国家对另一个国家的信息攻击能不能构成侵略行为？受到攻击的国家能否使用信息攻击以外的武力方法进行自卫？安理会能否决定对进行侵略、破坏和平、威胁和平的国家采取信息攻击？哪些信息战的手段与方法不允许使用？在信息战中如何区分军事目标和非军事目标？如何权衡对非军事目标的附带损害？在信息战中如何处理与非交战国的关系？”[4](P107-108)笔者认为还有：1. 战争与和平界限难分，战争的出现可能无任何征兆，战争的时间可能以分、秒计算。宣战不是根本不会出现，就是变得毫无意义。在战争开始前，一方就开始对敌方政治、经济、文化、科技等领域采取信息攻击，如在向他国出口武器装备中设置“后门”、“漏洞”以便以后瘫痪敌方；又如攻击敌方的通信、交通、电力网络。2. 军人与平民难以分辨，被攻击者难以分辨攻击者是自愿参与的黑客，还是敌方招募组织的“网军”。网络战进攻容易，也隐蔽。3. 网络战可不“战”而屈人之兵。战争可能不费一枪一弹、不动一兵一卒，敌方指挥控制系统网络已瘫痪，看不见敌方痛苦、牺牲、战争的残酷和生态环境破坏。4. 军事设施和民用物体难以分辨，如美国军用网络与民用网络紧密联为一体，互相交叉、共享信息。5. 前方与后方不分，只要存在网络的地点就可以实施网络战。作战区域广大，局势的发展不受交战任何一方的控制，非交战国的权益如何维护？6. 现行战争法确立的“禁止使用将引起过分伤害和不必要痛苦的作战手段、作战方法”原则、“区分军人与平民、军事设施和民用物体，不打击非军事目标”原则、“尽量减少对平民的附带损害，禁止不分皂白的攻击”原则等等原则难以适用、有效约束。7. 敌对方不占领土，保护战俘、伤病员的人道主义原则失去了意义，中立原则适用困难。8.《海牙第四公约》中约束法无明文规定的“马尔顿条款”不能适用网络战，1998 年通过的《国际刑事法院罗马规约》和其《犯罪要件终结案文》、《程序和证据规则终结案文》中有关战争罪的条文、程序和证据规则也基本不能适用网络战。

总之，网络战将改变未来作战形态，现行战争法的严重滞后使其对网络战的调整形成了法律“真空”，网络战从根本上颠覆了现行战争法，美国的绝对领先也对实现多极化世界不利，笔者提议国际社会高度关注这一危及人类社会的亟待解决的问题，尽快补充和完善现行战争法来限制发动信息战。

三、如何补充和完善现行战争法以应对网络战

补充和完善现行战争法以应对网络战要针对网络战的形式和特点，立法要有创新思维、有预见、超前，要使立法能准确反映、指导现实，要具体、明确全面。

1. 要严格限制发动信息战。各国对网络战“瞬间毁灭”忧心忡忡，争夺“制网权”、“制信息权”的新一轮军备竞赛已在全球展开。故要国际社会立法严格限制进行信息战。要明确网络战的概念、可使用的武器、作战手段、作战方法、允许的作战范围，还要严格限制进行信息战的实验。要明确限制使用的作战工具。国际社会可制定一项国际性的网络武器限制公约或国际互联网安全公约。

2. 要明确规定发起网络战要宣战，不许“先发制人”。“先发制人”在现行战争法中并未取得合法性，

后患无穷, 在网络战中更不行。

3. 要坚持人道主义原则, 对平民、非军事目标做出区分。当前一国各个关键性部门、产业和领域正在被网络联为一体, 形成信息化国家“关键性基础设施”, 信息安全已上升为一个事关国家政治、经济、军事、文化、科技、社会等各方面的核心问题。对一个信息系统发达国家的信息攻击会给其他国家的信息系统带来或大或小的危害, 并可能导致全球范围的灾难性后果。不能扩大作战范围。

4. 受到攻击的国家要确定发起网络战进攻的来源、对象和性质, 要区分犯罪分子、恐怖主义组织、黑客的信息攻击与国家指挥、控制的网络战。不能因犯罪分子、恐怖主义组织、黑客的信息攻击对他国发起网络战。因为个人、团体的行为在无充足证据证明其可归因于国家(如受某国家指挥、控制) 前, 在性质上不是国家行为, 而只是国际法上的“非国家行动者”的行为, 国家不承担国际责任。

5. 要明确规定受害国能否使用信息攻击或信息攻击以外的武力方法进行自卫。受害国可采取自保措施, 但不应任意报复, 要由联合国安理会决定能否对进行侵略、破坏和平、威胁和平的国家采取信息攻击。

6. 要明确谴责发起网络战的国家, 要明确规定不法行为的责任和赔偿责任。要修改 1998 年通过的《国际刑事法院罗马规约》和《犯罪要件终结案文》、《程序和证据规则终结案文》, 使犯罪要件、程序和证据规则能适用网络战, 让发动信息战的战犯能受到国际刑事法院惩处。

需要指出的是, 补充和完善现行战争法以应对网络战可能阻力重重。如同外层空间非战争化的立法。美国只许州官放火, 不许百姓点灯。美国控制了互联网的核心技术: 中央处理器 CPU、操作系统 Windows、基本浏览器 IE 和 Netscape, 掌握了绝对的垄断权; 美国把它主创的域名注册标准和传输协议 ICP/TP 等作为全球性的互联网工作标准向全球推广; 全球网民赖以生存的 13 台顶级域名服务器中, 仅有 3 台在美国以外; 85% 以上的网站用英文。[5](P393- 394)美国要利用垄断地位和实力优势为己谋取霸权和利益, 不愿受约束。即使立法, 也要竭力主导制定扩大其权利和行动自由限制他国权利和行动自由的规则。欧、日等西方国家也是如此。故各国难以达成书面协议。一些弱国、穷国特别是与美敌对的国家心存他念, 认为网络战消耗成本低, 付出的代价低, 但收效极大。

在缺乏最高统一立法机关的国际社会里, 为加速战争法的完善, 需要进一步发挥联合国国际法委员会编纂工作的创造性功能。国际法委员会应从维护全人类共同利益出发, 加紧调查研究工作, 集思广益, 尽快编纂建议性草案供各国讨论。之后联合国要积极敦促各国发表意见, 协调分歧、尽快达成广泛共识, 进而缔结国际条约。它本身可以通过联合国大会决议或安理会决议进行国际立法, 也可仿效“使用核武器是否合法案”请求国际法院发表咨询意见。国际人道主义机构如国际红十字会国际委员会、红十字会与红新月会国际联合会也可提出建议性草案。“此外, 在各国难以达成书面协议的某些人类活动, 由一些国家率先在某些事项上从事的实践活动因为符合其他国家的利益和需要, 从而为其他国家所接受和仿效, 在此基础上也可产生习惯国际法规则。”[6](P10)联合国和世界大多数爱好和平的国家要当仁不让、未雨绸缪, 加强合作以解决网络战无法可依的困境, 补充和完善因现行战争法滞后带来的法律真空, 将信息战这匹野马套上缰绳。我国身为安理会常任理事国有资格向联合国提出议案, 把限制网络战的内容增加到《联合国宪章》中, 督促联合国大会或安理会作出决议限制。可喜的是, 在联合国和世界大多数爱好和平的国家的艰苦努力下, 打击网络恐怖主义的国际条约(如欧洲关于网络犯罪的公约) 已通过, 相信国际社会尽快就比网络恐怖主义危害更大的网络战达成共识。

参考文献:

[1] 宋国涛等. 中国国际环境问题报告[M]. 北京: 中国社会科学出版社, 2002.

[2] 环球时报. 北京. 第 978 期 2005 年 6 月 1 日, 第 984 期 2005 年 6 月 15 日.

[3] 张全义. 当代世界政治经济热点问题[M]. 杭州: 浙江大学出版社, 2003.

[4] 盛红生等. 武力的边界[M]. 北京: 时事出版社, 2003.

[5] 李维亮等. 动荡中的秩序[M]. 兰州: 兰州大学出版社, 2003.

[6] 中国国际法学精萃(2002) [M]. 北京: 机械工业出版社, 2003.

(责任编辑: 周文升)