

论网络战及战争法的适用问题^{*}

李伯军^{**}

内容提要: 一直以来, 人类科技的飞速发展对战争法的冲击和影响是巨大的。进入 21 世纪以来, 互联网在得到迅猛发展的同时, 基于网络攻击行为而被视为网络战的事例时有发生。由于互联网超越了传统国家领土边界的限制, 因而使得战争法在适用于网络战的过程中引发了诸多法律问题。其中一个非常重要的问题是, 战争法规则能否适用于网络战当中? 学界对此存在争议。因此, 尝试解释和澄清这一问题有助于我们应对 21 世纪包括网络战在内的信息化战争对国际法所带来的诸多挑战。

关键词: 网络战 武力攻击 自卫权 战争法 国际法

近年来, “网络战”这一术语频频出现于新闻报道、学术著作之中, 同时也为各国军方所经常援引。不过, 我们不应应对近年来有关“网络战”、“信息战”的提法及实践感到陌生和惊讶。一个基本的事实是, 现代互联网本身最早就是从美国军方内部网络发展起来而后进入民用领域的。国际社会最早关注网络战始于 20 世纪 80 年代美国军方计算机遭遇病毒入侵事件。1988 年 11 月 2 日, 美国国防部战略 C4I 系统的计算机主控中心和各级指挥中心相继遭到计算机病毒入侵, 共造成约 8500 台军用计算机被感染病毒, 其中 6000 台无法正常运转。从此, 国际社会发生的有关网络战事件接连不断: 1990 年海湾战争期间, 美国中情局特工在开战前将带有病毒程序的芯片植入到伊拉克防空系统, 导致其不能正常运转, 从而为美国空袭伊拉克创造了条件; 在 1999 年科索沃战争中, 南联盟利用病毒对北约计算机网络系统发动了攻击, 而北约则以相同的方式进行网络反击; 从 2001 年到 2002 年期间, 英国黑客加里·麦金农非法侵入美国国防部、国家航空和航天局等多个部门的 97 部计算机; 2002 年夏天, 在克什米尔地区冲突中, 一个名为“g 力量”的巴基斯坦黑客组织侵入了印度国防部网站, 并篡改了印度国防部网站部分内容; 2005 年 5 月 10 日, 一个瑞典籍年轻人因实施了有关秘密侵入美国军方及宇航局网站在内的数千计算机系统的网络犯罪行为而接受美国警方审讯; 2007 年 4 月 27 日, 爱沙尼亚重要的政府、银行、媒体网站都遭遇空前的黑客攻击, 甚至一度被迫关闭; 2008 年 8 月, 受“南奥塞梯事件”的影响, 俄罗斯先行攻击并控制了格鲁吉亚的网络系统, 使格鲁吉亚的交通、通讯、媒体和金融等互联网服务系统瘫痪, 从而为自己顺利开展军事行动打开了通道; 2009 年 1 月, 法国海军内部计算机系统的一台电脑遭受病毒入侵, 并迅速扩散到整个网络, 导致网络一度不能启动, 海军全部战斗机也因无法下载飞行指令而停飞两天; 2011 年利比亚战争期间, 为重点攻击卡扎菲政权位于的黎波里的政府部门和部队, 西方联军局部入侵了利比亚网络, 并干扰了其通信和雷达系统。

对于上述事件, 我们可能感到眼花缭乱。不过, 几个关键技术或许可以为我们理顺这些事件之间的相互关系和影响提供某种有益的思路: “网路战”、“黑客”、“网络攻击”、“黑客攻击”、“网络犯罪”等, 其中最震撼我们眼球的一个概念便是“网络战”这一术语。在这里, 我们需要提出的一个非常重要的问题是“网络战”时代真的已经来临了吗? 对于这个问题的回答, 美国其实是最有发言权的一个国家, “因为美国是世界上第一个提出网络战概念的国家, 也是第一个将其应用于实战的国家, 目前, 美国军方在全球 88 个国家和地区的 4000 多个军事基地内, 拥有超过 1.5 万个电脑网络和大约 700 万台计算机。”^①2009 年 6 月 23 日, 美国国防

* 本文受教育部人文社会科学研究青年项目“联合国集体安全制度面临的新挑战”(项目批准号: 09YJC820098) 和教育部人文社会科学重点研究基地重大项目“全球安全基本法律问题研究”(项目批准号: 12JJD820004) 的资助。

** 湘潭大学法学院副教授, 湘潭大学战争与武装冲突法研究中心主任, 法学博士。

① 杨玉国《美国网军司令将制定网络交战规则》, 载 2010 年 6 月 9 日《长江日报》。

部部长盖茨正式宣布成立美军第 11 个司令部——“网络战司令部”,国家安全局长基思·亚历山大四星上将将被提名担任司令。在美国的示范下,近年来,英国、中国、以色列、俄罗斯、韩国、日本、印度、朝鲜、德国、伊朗等国也都已经开始纷纷建立自己的网络战部队,以应对现在和未来可能发生的网络战。

在上述背景下,值得我们探讨的一系列问题包括:到底什么是网络战?网络攻击能否构成国际法上的“武力攻击”?如果成立,受网络武力攻击的国家又该如何合法地行使自卫权?而更为重要的是,现有的战争法能否适用于网络战?

一、“网络战”及其相关概念的厘定

1993 年,美国兰德公司的阿尔奎拉和伦费尔特发表了题为《网络战要来了》的论文,第一次正式提出了网络战的概念,认为网络战是“为干扰、破坏敌方网络信息系统,并保证己方网络信息系统的正常运行而采取的一系列网络攻防行动”,是“21 世纪的闪电战”。^② 尽管时下人们对于“网络战”的讨论比较热烈,但对于到底什么是网络战问题的讨论却显得非常混乱。诸如“网络战”(Cyber Warfare)、“信息战”(Information Warfare)、“网络攻击”(Cyber Attack)、“计算机网络攻击”(Computer Network Attack)、“电子战”(Electronic Warfare)等术语经常被学者们所交替使用。因此,对于上述有关概念的厘定是非常重要的,因为这关乎到本文后续有关讨论的展开与结论的做出。事实上,以上术语词之间存在一定的差别。

所谓网络攻击,一般是指“计算机网络攻击”,即有关网络使用者利用一方网络存在的既定漏洞和安全缺陷对其网络系统和资源进行的入侵和破坏等行为。而网络攻击的发生并不一定意味着会发生网络战。网络战是指敌对双方针对战争可利用的信息和网络环境,围绕信息权的争夺,通过计算机网络在保证己方信息和网络系统安全的同时,扰乱、破坏与威胁对方的信息和网络系统。从本质上讲,网络战是信息战的一种特殊形式,是在网络空间上进行的一种作战行动。与传统战争相比,网络战具有突然性、隐蔽性、不对称性和代价低、参与性强等特点。^③ 还有学者从对控制计算机网络信息的角度来界定网络战,认为网络战是指为干扰、破坏敌方网络化信息系统并保证己方网络化信息系统的正常运行而采取的一系列行动,目的是夺取或保持信息优势或控制信息权。^④ 也有学者将网络战纯粹理解为敌我双方对于网络的相互破坏行为,即网络战是为干扰、破坏敌方网络信息系统,并保证己方网络信息系统正常运行而采取的一系列网络攻防行动。其作战样式包括:网络盗窃战、网络舆论战、网络摧毁战。^⑤ 因此,如果我们从狭义上来理解网络战的话,那么,可以看出,上述不同学者对于网络战的界定都有一个共同点,即都把网络战视为各国在战争中对网络的控制与利用的斗争。另外,我们还需要区分网络战、信息战与电子战这三个概念。信息战是指战场敌对方之间为保持自身对信息的获取权、控制权以及使用权而对对方开展的一系列敌对活动,其内涵和外延要比网络战更广,它可以包括网络战、情报战、电子战、心理战等。电子战一般是指敌对双方争夺电磁频谱使用权和控制权的军事斗争,具体表现为敌对双方互相进行电子侦察、电子干扰、电子欺骗、电子隐身、电子摧毁等方面的斗争。

综上所述,信息战其实包括了网络战和电子战。“网络战”和“电子战”都是与传统意义上的“海战”、“陆战”或“空战”这几个词处于同一层次上的一个概念,即都是发生于某个特定战场空间环境中的战争。所以,有相当一部分人提出了这样一个问题,即网络战是否是继陆、海、空、天、电之后的“第六空间战争”?然而,网络战不同于海战、陆战和空战的是,它可以被运用到海战、陆战和空战当中去。因而,当我们谈论网络战时,论及的既不仅仅是有关网络新武器这种新的作战手段问题,也不仅仅是有关如何人道使用诸多网络新武器的作战方法问题,而是一个全新的作战领域——网络空间。

二、“网络攻击”与国际法上武力的使用

可以确定的是,网络战的发生一般应是基于网络攻击而产生的。然而,网络攻击的发生并不必然带来网络战的发生,因为互联网上的普通网络攻击是一种受国内法管辖的普通刑事犯罪行为,实际上,网络中大部

② 参见龚新华、韵力宇《网络战,用看不见的方式摧毁你》,载 2011 年 1 月 14 日《中国青年报》。

③ 参见钱逢水《解读信息战、网络战、网络中心战》,载 2004 年 7 月 22 日《中国国防报》。

④ 参见褚法宝等《新概念武器与信息化战争》,国防工业出版社 2008 年版,第 25 页。

⑤ 参见苏进昌、王东华《网络在利比亚战争中扮演了什么角色》,载 2011 年 10 月 14 日《中国青年报》。

分攻击行为属于犯罪或间谍行为。除非这种网络攻击能构成国际法上的“武力攻击”。遗憾的是,现有国际法对于“武力攻击”这个词并没有做出明确的界定。^⑥ 笔者以为,网络攻击能否被视为武力攻击,这主要取决于我们对“武力”一词在现有国际法框架下的恰当解释。

对于“武力”这个词的有关解释,我们不得不提到1945年《联合国宪章》第2条第4款的规定,因为这是我们理解国际法上有关武力使用问题的一个关键性条款。而围绕该条款关于武力使用的解释问题,目前在学界出现了两种针锋相对的观点:一是主张武力仅指武装力量,二是主张武力不但包括武装力量,也包括胁迫等方式的非武装力量。^⑦ 目前,学界占主导性的观点和有关国家实践都支持了狭义上武力的概念,因为如果采用广义上武力的标准可能会引发国家行使自卫权的混乱,也不利于国际社会的和平与安全,还可能导致一方针对另一方之非武装力量的攻击而使用武装力量来进行自卫还击情况的发生。另外,很明显的是,宪章第2条第4款中“各会员国在其国际关系上不得使用威胁或武力”与“以与联合国宗旨不符之任何其他方法”的规定是选择性的,而且都共同指向“侵害任何会员国或国家之领土完整或政治独立”,这实际已经明确表明了该条款对“武力或威胁”与“其他胁迫形式”的区分。因此,国际法上的武力一般应该仅指“武装力量”。武装力量一般是指国家或政治集团基于自身防卫需要而配备一定的武器组成的各类组织。这里的关键问题就在于,像诸如“逻辑炸弹”(Logical Bomb)、“木马病毒”(Trojan)、“僵尸网络”(Botnet)以及“间谍软件”(Spy Software)等网络武器能否纳入国际法传统意义上的武器范畴?对此,学界还存在一定的争议,因为国际法对于什么是武器这个问题本身并没有做出规定。如有学者就指出,国际上一致认为,禁止使用武力除了应包括传统武器,还应包括细菌武器、生物武器、化学武器以及热核武器等。^⑧ 尽管如此,关于信息战的设备,诸如“Trojan Horse”、“Viruses”、“Worms”、“Sniffer”是否被同时代的国际法规则赋予暴力武器的资格,这个分歧依然存在。……基于当今一个政府可以用跨国信息战设备,通过网络空间对另外一个国家以网络为基础的设备进行破坏的事实,建议可以对使用武力的国际法规则进行更为宽泛的解释。^⑨ 如果说传统意义上的武器都具有可视性、爆炸性、物理破坏性等特征,那么,按照上述观点,网络攻击者所采用的网络武器是否一定要具备传统意义上的武器特征呢?

一般认为,武装力量所涉及到的武器是否一定具有传统意义上的爆炸性或物理破坏性没有必要考察。1996年国际法院在关于以使用核武器相威胁或使用核武器合法性问题的咨询意见中强调,在《联合国宪章》有关使用威胁或武力的条款中,关于一般禁止使用威胁或武力的第2条,关于承认每个国家有权实行单独或集体自卫权的第51条以及关于授权安理会采取军事措施的第42条等都没有提及特定的武器,它们适用于任何武力的使用,无论使用的是什么武器。《联合国宪章》也并没有明确地禁止或允许任何特定武器的使用,包括核武器。但一种武器使用的本身若是非法的,也不能以它是用《联合国宪章》所述的合法目的为由使它的使用成为合法。^⑩ 有学者指出,武器的技术水平影响了武器的形态,应当依据武器技术的发展水平来更新对“武装”的认识,否则人们对《联合国宪章》第2(4)条“武力”的理解将永远停留在二战结束时的水平,

⑥ 有关计算机网络攻击与使用武力的关系问题的论述可参见 Matthew C. Waxman, Cyber - Attacks and the Use of Force: Back to the Future of Article 2(4), in Yale Journal of International Law, Vol. 36, 2011; Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, in Columbia Journal of Transnational Law, Vol. 37, 1999; Daniel B. Sliver, Computer Network Attack as a Use of Force under Article, in INT'L L. STUD. Vol. 73, 2002; Jason Barkham, Information Warfare and International Law on the Use of Force, in International Law and Politics, Vol. 34, 2001; Matthew Hoisington, Cyber Warfare and the Use of Force Giving Rise to the Right of Self - Defense, in Boston College International and Comparative Law Review, Volume 32, 2009.

⑦ 关于对国际法上“武力”一词的解释问题可详见黄瑶《论禁止使用武力原则——联合国宪章第2条第4项法理分析》,北京大学出版社2003年版,第167-193页。

⑧ 参见徐军华《非致命武器使用的合法性与合理性分析——以国际人道法为视角》,载《法学评论》2010年第5期。

⑨ See Christopher C. Joyner and Catherrine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, in European Journal of International Law, Vol. 12, No. 5, 2001, pp. 845 - 846.

⑩ See Legality of the Threat or Use of Nuclear Weapons, Paras. 39, 41, I. C. J., July 8, 1996.

而与现代武器装备技术无关。^① 一个国家政府或其军队通过使用各种网络武器对他国发动网络攻击应该属于国际法上使用武力的行为,但这种攻击行为并不一定构成《联合国宪章》第51条中的“武力攻击”行为,因为通过支持一国反政府武装而间接使用武力的行为一般只能被视为是违反了国际法上的不干涉内政原则的行为,这点得到了1986年国际法院在尼加拉瓜案中所做判决的支持。国际法院认为,武力攻击概念不包括“以提供武器、后勤或其他支持的形式对反政府力量的协助”,^②“这种协助可被视为武力威胁或使用武力,或等同于对他国对内或对外事务的干涉。”^③因此,至少可以明确的是,一国对他国进行的网络攻击是对该国的内部事务的干涉,因而违反了国际法上的不干涉内政原则。

三、战争法适用于网络战的必要性及面临的困境

应该指出,“国际人道法只适用于在武装冲突(无论其为国家间、国家与有组织的武装团体间、还是各武装团体间发生的武装冲突)背景下实施的网络行动。我们需要把一般意义上的网络安全问题和武装冲突中的网络行动这一特定问题加以区别。‘网络攻击’,甚至‘网络恐怖主义’等词汇可能让人想到作战方法,但这些用词所指的行动并不一定发生在武装冲突期间。通过网络行动实施的犯罪活动可能并且的确发生在与战争状态完全无关的日常生活当中。在人们称之为‘网络攻击’的行动当中,很大一部分实际上是利用网络实现非法搜集信息的目的,并非发生在武装冲突的背景下。但在武装冲突局面当中,如果冲突方使用了基于网络行动的作战手段和方法,那么国际人道法就可以适用。”^④还有,在实践中,武力攻击既可以是零星的,也可是成规模的。这点也为国际法院在1986年尼加拉瓜案中所支持,即“武力攻击无需采取大规模军事行动”。^⑤因此,一般认为,零星、小规模的网络攻击行为及其反网络攻击行为不能认为是网络武装冲突,而必须是有组织的、大规模的、破坏严重的网络相互攻击行为才能构成真正意义上的武装冲突。由此看来,网络攻击以及其所引发的自卫并不必然导致武装冲突的发生,从而也并不必然导致战争法的适用。然而,一旦这种网络攻防是有组织、大规模、破坏严重的行为,冲突各方需要适用战争法的可能性就大大增加了。

(一) 战争法适用于网络战的必要性

显而易见,对于网络战所带来的巨大破坏性,没有人会感到怀疑。然而,要说网络战的非人道性,可能有一部分人会持反对意见,因为网络武器的使用并没有导致看得见、摸得着的“血淋淋”的后果,即网络战并不必然带来常规战争那样的以牺牲大量生命为代价的非人道后果,因而人道悲剧性并不十分明显,在这种情况下也就没多大必要适用战争法。这种观点其实只是抓住了问题的表象,因为网络武器足可以导致一个高度依赖网络的国家的军事、社会、经济体系之瞬间瘫痪,其破坏性并不亚于常规战争带来的破坏性,而且,网络武器同样可以通过篡改他国军方导弹参数和数据的方式而遥控发射,进而引发如传统战争那样的灾难性后果。依据1949年《日内瓦四公约》共同第2条以及1977年《日内瓦公约第一附加议定书》第1条和第96条的规定,不管交战各方是否宣战,也不管其是否承认战争状态的存在,只要存在武装冲突,作为各个缔约国和非缔约国(临时同意适用公约)的交战各方就必须适用和遵守战争法。因此,任何形式的战争都要服从于国际法和战争法的制约,虽然对于网络战,战争法缺乏针对性的具体规定,但其内在精神(如人道主义等)和基本原则(如区分原则、比例原则和限制原则等),可以适用于一切战争样式,网络战中各交战方也同样应当予以尊重和遵守。另外,按照马尔顿斯条款的规定,即使是在条约没有规定的情况下,也不能解除有关冲突方必须尊重国际人道法的义务。换句话讲,就是在国际人道法尚无具体规定的情况下,有关冲突方也不能为所欲为。如果考虑到在现代社会里,军事和新武器方面的科学技术的发展,要比法律的发展更为迅速,而法律条

^① 参见朱雁新《计算机网络攻击构成“使用武力”之分析》,载《战略机遇与军事法治的创新发展——以完善中国特色社会主义法律体系为背景会议论文集》,第221页。

^② See Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of 27 June 1986, I. C. J. Reports, para. 195.

^③ 前注^② para. 230.

^④ [瑞士]克尔杜拉·德勒格《网络空间并不存在法律真空》,http://www.icrc.org/WEB/CHI/sitechi0.nsf/html/cyber-warfare-interview-2011-08-16.

^⑤ 前注^② para. 195.

文上的制定往往要落后一点的情况,马尔顿斯条款原则具有特别重要的意义。^{①⑥}

(二) 战争法适用于网络战所面临的困境

如上所述,网络战带来的破坏性和严重性丝毫不亚于常规武器战争所带来的类似后果,这从很大程度上带来了战争法适用的必要性,同时也给传统战争法的适用带来了法律上的困境。有人对网络战与传统战争的特点之差异做了如下全面而恰当的对比:

“随着信息技术日新月异,网络战也越来越呈现出与传统战争不同的特点。首先,网络战的作战时空更加广阔。网络战不受时空条件限制,随时随地都有可能发生。网络覆盖的地方都在作战半径之中,所有的网络用户都可能为作战目标。而且,网络战可以瞬间完成作战目标、方向、兵力、地域的改变,攻防界限难以划分,传统的前方、后方、前沿、纵深等概念变得模糊。也就是说,网络战可以通过国际互联网将作战区域扩展到世界上任何网络可以到达的地方。其次,网络战的作战方式更加灵活。一般来讲,狭义网络战注重对网络系统的‘硬摧毁’(即物理上的消灭)^{①⑦}和‘软杀伤’(即用黑客手段进行攻击和破坏)。广义网络战则更注重依托网络进行渗透或干扰破坏,从经济、文化等方面进行渗透和价值观输入,发布或扩散各种对竞争对手不利的信息或假情报等。另外,与其他战争样式相比,网络战的作战手段也更加隐蔽。除了各种看起来高深莫测的网络攻击技术,例如病毒、蠕虫、木马、逻辑炸弹、拒绝服务攻击、信息篡改、电磁干扰以及端口扫描、IP欺骗、网络监听等手段外,现代间谍窃密的一个典型方式就是‘公开信息搜集’。”^{①⑧}

因此,依据网络战不同于传统战争的特点,我们实际可以发现:战争法适用于网络战将面临以下两个主要的困境:

1. 网络战中交战方主体与中立方主体身份难以确定。所谓战争法,它是指调整战争或武装冲突中交战方之间和交战国与中立国或非交战国之间关系以及作战方法和手段所形成的原则、规则和制度。因此,战争法存在的意义在于保护交战国、中立国、非交战国的交战秩序、合法权益以及保护各参战人员和战争受难者在战争中最低限度的人权。在网络战中,国家要抵御来自他国的网络攻击需要采取诸多防范措施,在技术上要求其不断升级自身的网络防御系统,并时刻保持警戒状态,因而在实践中实际很难、很好地防御网络攻击行为。网络攻防往往是瞬间完成,这种攻防的不断转换将导致自卫与网络攻击的频繁转换,将很难适用国际法和战争法的一些具体规则。而且,网络武器尤其是病毒性武器一旦发作,将不可能如实战武器那样容易控制,势必会波及和传染给任意国家的电脑系统,导致战场范围的不断扩大。在这种情况下,谁是交战方?谁是中立方?交战方和中立方的地位如何确定?这些问题在网络战的环境中将变得很难回答。美国SANS网络预警中心主任马库斯·萨科斯(Marchs Sachs)就曾经指出,“身份无法验证,让建立法律、监管或协议都很困难。如果有一天真的发生网络战,现在的《日内瓦公约》将无法适用,因为很难确定交战方是谁。”^{①⑨}另外,同样难以确定的问题是,谁是战斗员?谁是非战斗员?战斗员和非战斗员法律身份的界限如何划定?在上述这些问题无法回答的前提下,我们又如何能保护基于网络战当中战争受难者的最低限度的基本人权呢?

2. 战争法基本原则在网络战中将变得难以适用。战争法的基本原则主要包括人道保护原则、限制原则、比例原则和区分原则等,这些基本原则在网络战中适用时也存在诸多困难,其中以区分原则体现得最为明显。区分原则实际意味着在计划和实施网络攻击行动的过程中,国际人道法唯一许可攻击的目标就是军事目标,如为军事基础设施或明确用于军事目的的基础设施提供支持的计算机或计算机系统。因此,通过网络空间发动的攻击,其对象不可以是用于纯民用设施(如医疗设施、学校及其他纯民用设施)的计算机系统。^{②⑩}1977年《日内瓦公约第一附加议定书》第48条对区分原则进行了阐释,即武装冲突各方应当在平民居民和战斗员之间和在民用物体和军事目标之间加以区别,军事行动仅应以军事目标(人员或物体)为对象。区分

^{①⑥} 参见朱文奇《美伊战争与国际人道法》,载《政法论坛》2003年第4期。

^{①⑦} “硬摧毁”就是指攻击者运用电磁脉冲弹、次声波武器、高功率微波武器等对敌方网络进行物理攻击和破坏。

^{①⑧} 前注② 龚新华、韵力宇文。

^{①⑨} 转引自蒲实《网络战:安全威胁有多真实》,载《三联生活周刊》2010年第19期。

^{②⑩} 参见前注①④,[瑞士]克尔杜拉·德勒格文。

原则源于国际人道法最基本的一个概念,即:在武装冲突时期只有削弱敌方军事实力的作战手段才是可接受的。^{②①}然而,国际法并未明确战争期间各国怎样使用网络武器,海牙公约和日内瓦公约要求减少战争损失,因此,网络战争不得不区分军事目标与民用目标,因为个人计算机网络不受此限。^{②②}一个目标之所以成为军事目标并不是由其原有特征决定的,而是由敌方对其的使用,或该物体成为军事目标对攻击方的潜在利用价值而决定的。除受特别保护外的所有物体都有可能成为合法的攻击目标。因此,不可能将所有的军事目标完整地列一份清单,虽然如果真有这样一份清单,规则的实际执行就会变得简单得多。^{②③}而且,还需注意的一个问题是,攻击者身份的确认和军事目标的选择都是网络战中各个交战方军队依据自身的判断来做出的,此举进而将引发两个问题:一是在网络环境中确定攻击者的身份往往需要一定的时间,并不能马上完成,这样将会产生“事后报复”是否符合国际法规定的问题,因为自卫一般只能在遭受武力攻击的当儿采取。二是网络战中交战一方如果发生误判而导致其所选择的攻击对象错误的话,那么将不可避免地引发一系列的不可预测之严重后果。而且,在网络战中,当区分原则面对军民两用物体时将变得更难适用,因为“在高科技时代,计算机硬件和软件的建设对军事而言是不可或缺的,而且几乎不可能去确定某项技术是专为军事目的设计的,还是可以为军事目的所利用的。当某个物体既可用于军事目的又可用于民用目的时,人们可能会认为即使是间接地被用于军事目的也应被视为军事目标。然而,如果干扰了平民对某一物体的使用意味着给平民带来过度的损害,那么根据比例原则,对这一两用物体的攻击是非法的。”^{②④}

四、结论

总体而言,未来的网络战取决于三个方面的快速发展。一是互联网军事化。……随着网络技术的发展,以及它在各领域越来越广泛地应用,互联网有可能成为新的作战领域,即成为对立双方攻防的目标。二是物联网军事化。物联网是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把任何物品与互联网连接起来,进行信息交换和通讯,以实现智能化识别、定位、跟踪、监控和管理的一种网络。……三是无线联接技术。无线联接技术智能化和无线植入技术,是实现网络无限延伸的基础,是网络战拓展到陆、海、空、天、电以及各类武器装备的主要途径。^{②⑤}而且,网络战所关涉的国内法与国际法问题比较繁多和复杂,当我们真正倡导并将其付诸实施的时候必须高度审慎。因为网络战爆发时将引发一个不可控的风险,那就是弱国或小国可能凭借网络技术与与发达国家进行网络战的过程中取得某种优势,而发达国家则可通过网络之外的军事打击来进行报复,这样势必将危及现有联合国的集体安全制度,也将加剧战争法适用的复杂性。另外,现在依然存在的问题是:为了建立一个网络安全机制,在目前关于战争与和平的法律制度的基础之上,我们还应该需要哪些标准?由于网络战正处于初步阶段,有些人会认为,如果网络战不是一个不可能的挑战的话,调整它将是一个困难。然而,要避免所谓灾难性的网络攻击,作为一种威慑,不制定某些有关国际游戏规则将会显得很愚蠢和不切实际。^{②⑥}尽管网络战目前还处于初步阶段,但我们依然可以预见网络战的各种灾难性的后果,因此,必须事先达成有关国际合作。然而,我们也必须预见到这一过程的困难,因为正如 Scott J. Shackelford 教授所指出的,“不像其他诸如寻求禁止化学武器、生物武器以及核武器等军控条约那样,在现有国际法的框架下来禁止网络战的开展并不是一个简单的问题。这种困难根源于这样一个事实,即包括信息战在内的计算机网络代码经常和那些清白无辜的信息请求无异。”^{②⑦}

②① 参见朱文奇《国际人道法》,中国人民大学出版社2007年版,第91页。

②② See Tom Gjelten, Extending The Law Of War To Cyber Space, available at <http://www.npr.org/templates/story/story.php?storyId=130023318>.

②③ 参见[瑞士]马科·萨索利《当代武装冲突中的目标选择》,载《武装冲突法——现状、展望与训练:亚太地区武装冲突法研讨会文集》(2006年红十字国际委员会东亚地区代表处与中国人民解放军总政治部办公厅联合印刷),第103页。

②④ 前注②③,[瑞士]马科·萨索利文。

②⑤ 参见祁永强、王宁夏等《网络战威胁超越虚拟现实》,载2010年6月17日《人民日报》。

②⑥ See Dr Rex HUGHES, “Towards a Global Regime for Cyber Warfare”, available at http://www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf.

②⑦ See Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, in Berkley Journal of International Law, Vol. 25, No. 3, 2009, p. 216.

令人振奋的是,国际社会已经开始日益重视网络安全问题:2008 年 5 月,由马来西亚倡议建立的“国际反网络威胁多边伙伴联盟”(IMPACT)正计划就国际网络安全问题制订出一个为各国共同接受的准则或协议;2009 年 2 月 18 日,联合国秘书长安基文称联合国将考虑网络战及其对国际安全的影响和关键的现实问题;2010 年 7 月,由美国、中国、俄罗斯、英国、法国、德国、意大利、以色列、爱沙尼亚、白俄罗斯、巴西、印度、卡塔尔、韩国以及南非等 15 国签署了一份旨在减少网络攻击的协议。此外,15 国还提议,联合国应该出台规范网络空间行为的准则,对国家立法和网络安全战略交换信息,并且帮助不发达国家增强计算机体系的保护能力。看来,将日益严重的网络威胁与攻击行为或网络战纳入联合国框架范围内进行规制势在必行。网络攻击能允许国家和非国家行为体不通过诉诸传统的武力行为就可以对他国施加大规模伤害,但是,长期以来的一个真实情况是,包括经济、金融手段、隐晦的托辞以及其它被广泛运用的手段也可达到上述效果。在这点上,为了从法律上有效规制网络攻击,国际社会制定一项新的国际条约或国际协议而不是通过对联合国宪章的固有解释的做法的优点在于:如果任何有关努力都是基于扩大对联合国宪章法律的解释的话,其成效将是很微小的。然而,在单方面的国家实践还没有达成一致的情况下,通过加强对联合国宪章的解释工作而不是制定新的国际协议的一个优势在于:联合国宪章法律能逐步演变,并且可以对国际行为者的期望进行不断地塑造。^② 不过,笔者以为,鉴于网络空间环境的特殊性和复杂性以及顾及到个人安全与全球安全问题,未来国际社会适宜采取制订专门国际公约的办法来规范网络的普通攻击行为以及在网络环境下的具体作战行动问题。

(责任编辑:黄德明)

^② See Matthew C. Waxman, Cyber – Attacks and the Use of Force: Back to the Future of Article 2(4), in The Yale Journal of International Law, Vol. 36, 2011, p.453.