战争法在网络空间的适用性：探索与争鸣

徐龙第

近年来，网络安全事件层出不穷，安全形势日益严峻。为应对网络威胁，国际上关于制定网络安全规则的呼声和提议此起彼伏，接连不断。其中，现有战争法在网络空间的适用性问题便是当前国际讨论的热点之一。

网络活动性质各异，网络战存在与否仍存争议

一、网络活动性质各异

网络活动种类繁多，但其性质却有很大不同，人们对网络活动、网络威胁和网络安全的认识也存在差别。例如，有人认为，网络威胁可以分为网络侵入、有组织犯罪、意识形态和政治极端主义、国家发起的网络侵略等四个层次；也有人认为，网络攻击包括黑客行为、分布式拒绝服务（DDoS）、特洛伊木马等；还有人认为，网络攻击包括网络恐怖主义、网络战、网络犯罪、网络间谍等四种类型，其中，虽然恐怖主义组织在网上也有其存在形式，但真正的网络恐怖主义仍十分罕见，真正的网络战争也从未发生过。相反，最紧迫的问题是网络犯罪和网络间谍。鉴于网络活动复杂多变，网络威胁广泛存在，制定应对网络威胁、维护网络安全的规则势在必行。

网络战作为网络威胁和网络攻击的极端表现形式，正日益引起人们的广泛关注。实际上，自互联网诞生以来，国际上关于网络战的讨论和声音就不绝于耳，各国竞相争夺“制网权”。在1991年的海湾战争、1999年的科索沃战争、2003年的伊拉克战争中，网络工具都大显身手。许多国家近年来更是采取各种措施，纷纷出台网络政策，制定网络战略，建立网络司令部，加强网络建军，“网络战”似乎一触即发。近年发生的一些网络攻击事件进一步为网络战的到来提供了佐证，2007年爱沙尼亚受到的网络攻击和2010年发现的“震网”蠕虫病毒便被视为网络战的最新案例。前者被爱沙尼亚国防部长称为“没有被注意到的第三次世界大战”，西方网络战专家更是将其称之为真正意义上的第一场网络战。“震网”病毒虽未能摧毁伊朗核设施，但致使伊朗约20%的离心机就此报废，从而大大延迟了伊朗核计划。“震网”病毒的出现标志着又一种网络武器的诞生，网络战也进入了新阶段。

二、网络战存在与否仍存争议

人们对战争的定义与理解不同，对网络战的认识也有差异。总体而言，目前对网络战的存在与否尚无共识，大体可以分为两种观点。一种观点认为存在网络战，已经发生；另一种观点则认为不存在网络战，尚未发生。早在1993年，美国兰德公司的约翰·阿奎拉（John Arquilla）和戴维·朗菲尔德（David Ronfeldt）就宣称，“网络战来啦！”美国国防部副部长威廉·林恩三世（William Lynn Ⅲ）2010年写道，“尽管网络空间是一个人造领域”，但对军事行动来说，它已变得“和陆、海、空、天一样重要”。白宫的前网络“沙皇”理查德·克拉克（Richard Clarke）认为，网络战使“9·11”事件都显得相形见绌，并敦促采取大量措施，“以便现在就开始防止网络战的灾难”。2011年2月，时任中情局局长的莱昂·帕

内塔（Leon Panetta）更是发出警告，“下一个珍珠港很可能是一场网络攻击”。当然，有人认为这是一种“网络狂躁症”，是对网络攻击的过度反应。

与此“狂躁症”不同，伦敦国王学院的托马斯·里德（Thomas Rid）则认为，尽管有许多网络攻击发生，但网络战在历史上从未发生过，现在没有、将来也不可能发生。这是因为，一种进攻性行为必须满足某些条件才能构成战争行为。按照克劳塞维茨的定义，战争必须具备暴力性、工具性、政治性三个特点。或者说，任何战争行为都必须具有潜在的致命性、工具性和政治性。但是，在已经发生的网络攻击中，无论是较小或重大的网络攻击，尚无一起满足这些条件，也就不能构成战争行为。相反，所有过去和现在的政治性网络攻击都可以归为三种较为复杂的活动形式，即颠覆（subversion）、间谍（espionage）、破坏（sabotage），而它们与战争一样古老。

界定“网络战”需要考虑的几个维度

在对网络战概念尚无共识的情况下，厘清网络战的几个维度对准确界定和理解网络战将大有裨益，如攻击者和攻击目标、目的以及后果等。

一、攻击者和攻击目标

简单地说，攻击者可以分为个人、团体、国家三个层次的行为体。如果对之进行搭配，便可以结成不同的对子：个人←→个人、个人←→团体、个人←→国家、团体←→团体、团体←→国家、国家←→国家。就上述各个对子之间的搭配而言，只有国家←→国家之间的攻击才能被称为战争行为，而另外五个对子之间的攻击则很难被称为战争行为。当然，如果个人和团体得到国家的授意、授权或指使，也可以构成战争行为。然而，由于网络空间自身的特性，难以对网络攻击进行溯源，因此，也就很难确定攻击者，很难判定网络战的存在与否。

就攻击目标而言，通常包括计算机操作系统及软硬件；个人信息、商业机密、知识产权等软资源和计算机信息；银行、航空、交通、水利、大坝、电站等关键基础设施。这些目标可能属于个人、团体或国家的资产，所处的层次不同，所具有的价值不同，仅凭某个单一要素/维度很难确定网络战的存在与否。这也是从攻击者和攻击目标的角度界定网络战时所面临的难题。

二、网络攻击的目的和后果

与网络活动的种类一样，网络攻击的目的也是五花八门。有些完全是出于攻击者个人的兴趣和好奇心，或者是为了展示自己的计算机才华和才能，早期的“黑客”大都如此。有些是为了获取商业机密，谋取经济利益，甚至进行网络诈骗。有些是为了进行破坏活动，包括破坏和删除目标计算机的信息，破坏或瘫痪计算机的软件和操作系统，破坏计算机硬件或信息基础设施，等等。当然，还有些网络攻击是为了进行网络战，包括有限的和无限的网络战。

与此相应，不同目的的网络攻击，也会造成不同的后果。这些可能的后果包括：个人和商业信息的丢失，知识产权的被窃，计算机软硬件及操作系统的破坏，关键信息基础设施的摧毁，甚至是人员的伤亡，等等。除人员伤亡外，其余的后果在现实世界中都有发生，但它们却很难被视为构成网络战的要件。即使发生了人员伤亡的情况，还需要区分是直接伤亡，

还是间接伤亡。这些情况都会影响对网络战发生与否、存在与否的判断。

简言之，在分析和判断网络事件的性质时，应综合考虑各种要素，客观分析具体情况，包括网络攻击的主体、客体、目的以及可能的后果等，不应夸大或罔顾事实，避免把所有网络攻击一概归为战争行为，陷入网络战的简单化逻辑。

网络战的规范与战争法

一、如何规范网络空间冲突与战争

对网络战进行规范，无外乎两种办法：一是制定新的国际法规则，签订新的国际条约，如中国和俄罗斯等国提出的《信息安全国际行为准则》（以下简称《准则》）；二是调整现有国际法规范，使之适用于网络空间和网络战，这得到了美国和北约等西方国家和国际组织的支持。2011年9月12日，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦共同致信联合国秘书长潘基文，请其把《准则》作为第66届联大的正式文件散发，呼吁各国在联合国框架内讨论该文件，以尽早就涉及信息和网络空间的国际准则达成共识，规范国家行为。这是国际社会首次较为全面、系统地提出有关信息和网络安全国际准则的文件。然而，“美国及其西方盟国在很大程度上”对该《准则》草案“置之不理”。最近，卡特政府时期的高级顾问阿米塔伊·艾次奥尼（Amitai Etzioni）表示，“如果不知道是哪些国家提交了该提案，那么就会很容易地认为，该提案95%的内容是由美国领导的西方国家起草的”。这充分说明了《准则》的普遍意义。

与此相反，美国、北约等西方国家和国际组织认为，现有国际法可以适用于网络空间，无需另立新法。2012年9月，美国国务院韩裔法律顾问高洪柱（Harold Hongju Koh）在美国网络司令部的部门间法律会议上正式表达了这种立场。同月，北约在历时三年的研究之后，也发布了《关于国际法适用于网络战的塔林手册》（以下简称《手册》）。在编撰过程中，《手册》汇集了北约国家在国际法、国际关系、网络安全等领域的几十位专家，成员国政府也派代表作为观察员参与有关讨论。《手册》提出了适用于网络战的95条规则，涉及国家在网络空间的权利与责任、武力的使用等内容，并配有对每条规则的评论，反映了《手册》制定过程中的有关讨论、共识及分歧。作为一部指导手册，内容非常全面。当然，北约也表示《手册》并不代表其官方观点，而是各位专家的个人观点。在人们对网络战的存在与否仍然存在分歧的情况下，美国不仅明确认为现有国际法适用于网络空间，北约更是编撰了详细的指导手册，在规范网络战方面走得可谓相当超前。

二、战争法的双重目的

除《联合国宪章》（第2条、第51条）等规范武力使用合法性的规则之外，专门用于规范战争行为的国际法律规范还包括日内瓦四公约及其附加议定书，[1]亦即通常所谓的战争法，也被称为武装冲突法或国际人道主义法（IHL）。就网络空间而言，除制定专门用于网络战的国际规则外，便是要讨论战争法适用于网络空间的可能性。然而，这方面的许多讨论往往忽视了战争法的初始目的。

无论是制定关于网络战的新规则，还是把现有国际规范用于网络战，都不能忘记战争法的最初目的：一是保护那些没有或不再参加战斗的人（如平民、军队中的医务和宗教人员）

以及那些已经停止参加战斗的人（如受伤、遇船难和生病的战斗员以及俘虏）；二是限制作战手段（特别是武器）和作战方法（如军事战术），进而减轻武装冲突的影响。战争法禁止使用可导致下列后果的所有作战手段和方法：无法区分参战人员和未参战人员（如平民），其目的是保护平民居民、平民个人和平民财产；造成过分伤害或不必要痛苦；对环境造成严重或长期的损害。明确战争法的目的可以使有关讨论更加聚焦、集中，增强其针对性和目的性，进而提升其适用性和有效性。

战争法基本原则在网络空间的适用性及其困境

从战争法的双重目的来看，应当肯定战争法也可以适用于网络空间，即在网络战中保护非战斗人员以及限制网络武器。然而，把战争法基本原则用于网络空间时，也面临着一些困境。在具体运用战争法的基本原则时，便会出现许多难题。

一、网络战的门槛与合法自卫原则

《联合国宪章》第2条第4款规定，“各会员国在其国际关系上不得使用威胁或武力，或以与联合国宗旨不符之任何其他方法，侵害任何会员国或国家之领土完整或政治独立。”然而，在网络空间，什么样的网络攻击才算“使用武力”和“武装攻击”呢？这涉及到网络战的门槛问题，亦即什么样的网络攻击才算网络战。由于大部分恶意网络活动并非网络战，而是网络犯罪和网络间谍行为，因此，网络战的门槛应该高设，而非低设。否则，不仅会在概念上陷入混乱，致使各国应接不暇，在国际法的应用上也会陷入混乱。《宪章》第51条规定，联合国任何会员国受武力攻击时，在安全理事会采取必要办法以维持国际和平及安全以前，本宪章不得认为禁止行使单独或集体自卫之自然权利。然而，在网络空间进行自卫需要哪些条件？可以使用哪些手段进行自卫？能否使用常规武器进行报复？这些问题都需要进一步明确。而且，由于网络攻击具有匿名性、非对称性、即时性、突发性等特点，往往被视为弱者的武器，宣战原则要用于网络空间并非易事。否则，若进行宣战，网络攻击的效果将大打折扣。

二、区分原则和比例原则

根据战争法的区分原则，即使是网络攻击，原则上也应该只针对军用网络，应区分军事目标与非军事目标、民用设施与军用设施、战斗人员与非战斗人员、平民与武装部队。然而，在今天的网络世界中，要进行这种区分并不容易，因为网络基础设施往往大都是军民“两用”，不可能完全隔离开来。而且，攻击目标一旦确定，军人和平民都可以发起攻击，难以区分战斗人员与非战斗人员。比例原则要求军事行动造成的连带损害不能超过这种行动所可能带来的直接、具体的军事好处。在网络空间，虽然可以进行“精确定位”式的网络攻击，以尽量减少不必要的损害，评估网络攻击所可能带来的好处也尚属可能，但要限制网络攻击可能造成的连带损失则相当困难，因为这种连带影响可能涉及多个维度和层次，包括军事、经济、社会等多方面的影响，造成的后果往往难以估量。因此，作为一般性的战争法原则，区分原则和比例原则在网络攻击中应得到遵守，但在实际应用中将遇到不少难题。

三、中立原则和中立国的利益

国际法保护中立国的合法权益，在网络空间中亦不例外。如前所述，网络攻击的形式多种多样，而网络溯源却十分困难。分布式拒绝服务（DDoS）等类型的网络攻击需要动用大量的计算机参与其中，致使许多计算机网络在浑然不知的情况下成为他者用来实施网络攻击的“僵尸”网络。在网络战中，中立国的网络系统和资源也很容易被交战一方用来攻击另一方，而中立国却“浑然不知”。因此，一方面，中立国很容易成为网络攻击的“替罪羊”，而真正的攻击者却逍遥法外；另一方面，鉴于难以网络溯源的现实，在网络战中保护中立国的权益也就无从谈起。因此，中立原则用于网络空间时也面临着一定的困难。

四、网络主权原则

主权原则是当代国际体系和国际关系的基石和基本原则。无论是2010年6月中国政府发布的《中国互联网发展状况》白皮书以及前述的《信息安全国际行为准则》，还是联合国信息社会世界峰会2003年12月的《日内瓦原则宣言》以及2005年的《突尼斯议程》，都承认一国的网络主权。前述高洪柱在演讲中也认为，在网络空间开展活动的国家必须考虑其他国家的主权，包括在非武装冲突的背景下也是如此。他指出，支持互联网和网络活动的物理基础设施通常位于主权领土范围内，受所属领土国家的管辖；由于网络空间相互联系和兼容的性质，针对一国网络信息基础设施的行动可能在另一国产生影响；一国无论何时考虑在网络空间进行活动，都需要考虑其他国家的主权。北约的《塔林手册》认为，任何国家都不能对网络空间本身宣称拥有主权，各国可以对其领土内的任何网络基础设施及与其相关的活动行使主权，包括在其领土上从事网络活动的人员、位于其领土内的网络基础设施以及根据国际法所享有的“治外法权”。简言之，网络主权原则包括对一国领土内的互联网基础设施、个人和团体及其网络活动的管辖权，以及互联网公共政策的制定权等几个方面。网络主权原则使各国在网络空间处于同等地位，有利于各国维护自身网络安全与利益。理论上，各国在网络主权问题上应该比较容易达成共识，但在实践中，对网络主权内涵和内容的解读却可能存在差异。

五、战争法适用于网络战的情况

作为一个新领域，网络空间还存在着许多未知数，战争法应用于网络战时也面临着诸多难题。然而，这并不意味着国际法就不能适用于网络空间，也不意味着人们在新情况、新问题面前无动于衷，毫不作为。相反，为避免后见之明，我们应积极探索战争法在网络空间的适用性，而不是经过历史上的那种残酷战争之后才制定相关准则和行为规范。就此而言，除讨论战争法的哪些基本原则能够适用于网络空间之外，还应积极探索到底在哪些情况下战争法能够适用于网络空间。

在当前的诸多讨论中，似乎正逐渐出现一些共识：一是在发生战争的情况下，战争法是适用的；二是在造成重大人员伤亡的情况下，战争法也适用。在发生战争的情况下，网络战只是整体战争的一部分，网络也只是可资利用的战争工具和手段之一，战争法自然适用。而当前讨论较多的重大人员伤亡主要是指发生“网络珍珠港”、“网络9·11”那样的重大事件及其造成的人员伤亡。然而，到底什么样的人员伤亡才能称为重大伤亡，还需要更加深入

的讨论。

（作者系中国国际问题研究所欧洲研究部副研究员）

（责任编辑：张凯）

［1］四公约是指《改善战地武装部队伤者病者境遇之日内瓦公约》（第一公约）、《改善海上武装部队伤者病者及遇船难者境遇之日内瓦公约》（第二公约）、《关于战俘待遇之日内瓦公约》（第三公约）、《关于战时保护平民之日内瓦公约》（第四公约）。附加议定书包括第一附加议定书《1949年8月12日日内瓦四公约关于保护国际性武装冲突受难者的附加议定书》（1977年6月8日订立）、第二附加议定书《1949年8月12日日内瓦四公约关于保护非国际性武装冲突受难者的附加议定书》（1977年6月8日订立）、第三附加议定书《1949年8月12日日内瓦四公约关于采用新增标志性徽章的附加议定书》（2005年12月8日订立）。