《塔林手册》中有关网络战争的武力使用问题
——从国际法角度展开

季 华
（北京大学 法学院，北京 100871）

摘 要：禁止使用武力是《联合国宪章》第2条第4项明确规定的，也是一项强行国际法规则（jus cogens）。尽管《联合国宪章》没有确定“武力使用”的范畴，但根据条约解释规则，“武力”一词应被限定为军事力量。作为一部意图规制国际网络安全的文件——《塔林手册》，坚持将网络攻击等活动纳入到“武力使用”的范畴之内。手册既无法律约束力，也不是一项法律创制；手册本身对武力使用的定性存在法理缺陷和实践误读。《塔林手册》对武力使用的界定值得传统国际法规则回应和反思。

关键词：网络安全；网络战争；国际法；《塔林手册》；武力使用；《联合国宪章》
中图分类号：D99 **文章标识码**：A **文章编号**：1006-6152（2016）03-0028-07
DOI：10.16388/j.cnki.cn42-1843/c.2016.03.004

近年来，中美之间的“网络安全之争”备受关注。针对美国政府所称的“来自中方网络攻击”等问题，中国外交部在数个场合表明了中方对网络安全问题的立场[①]。网络安全虽不是个新话题，但在国际法话语中，网络属于较新且没有明确规则可适用的领域。2009年由北约卓越合作网络防卫中心（Cooperative Cyber Defense Center of Excellence，CCDCE）编制了全称为《适用于网络战争的塔林国际法手册》（简称为《塔林手册》），手册于2013年3月由剑桥大学出版社出版。

《塔林手册》一经出版，便引起国内外学界的关注和讨论。西方国际法学界对手册有截然不同的态度。比如以迈克尔·施密特（Michael Schmitt）为首的大多数美国学者认为网络安全完全可以从既有国际法规范中找到指引，网络攻击可以被认定为武力使用；欧洲主流国际法学界认为手册对既有国际法规范的移植在法理上存在着诸多缺陷，甚至是牵强附会的，比如网络自卫权的概念不清晰，并未形成习惯国际法等等。与此同时，国内学界主要对《塔林手册》采取一般的综述性研究，没有对手册单个国际法问题做深入探讨。《塔林手册》涉及的国际法律问题主要有“武力使用”“反措施”“自卫权”等。本文认为，在这些问题中最重要的国际法问题是手册第一部分认定的“武力使用”。首先，从手册的逻辑和体例上看，网络中的武力使用是一个前置议题。其次，按照《联合国宪章》第51条，联合国会员国若受到武力攻击可以享有自卫权。从这层意义上说，是否将网络攻击认定为“武力使用”，直接关系到受攻击国是否可以采取“反措施”甚至行使自卫权，而受攻击国一旦行使自卫权，所谓网络战争才有存在的基础。因此，笔者认为有必要对《塔林手册》第一部分认定的“武力使用”进行研究并作出回应。本文在认定手册没有一般国际法地位的前提下，认为《塔林手册》并非法律创制，而仅是对既存国际法规范的移植。更重要的是，本文将详细考察手册对“武力使用”的界定和立论基础，并得出手册的界定和立论基础不符合条约解释规则，曲解了国际司法实践本意这一结论。

一、《塔林手册》的制定及文本性质

围绕网络管控的讨论不是近几年的事。早在20世纪90年代，围绕网络战的法律规制讨论便已开始。《塔林手册》总编迈克尔·施密特在1999年发表了题为《计算机网络攻击和国际法上使用武力问题：基于规范框架的思考》一文[1]。文中提出了将

收稿日期：2015-12-07
作者简介：季 华，男，江苏盐城人，北京大学法学院博士生。
本刊网址·在线期刊：http://qks.jhun.edu.cn/jhxs

网络攻击视为武力使用的六点原则,这六点原则在后来的《塔林手册》第11条得以体现[2]。国际社会在发生一系列“网络攻击”事件后②,逐渐认识到必须要对网络攻击进行规制。在此背景下,2009年由CCDCE组织专家编制了《塔林手册》。《塔林手册》分为两大部分:第一部分为“国际网络安全法”,主要将国家主权、武力使用、自卫权等传统国际法规则移植到国际网络安全规则中;第二部分为“网络武装冲突法”,该部分将武装冲突法的内容映射到国际网络战争中,内容涉及网络作战人员的认定、网络攻击的认定、占领和中立规则等等。手册在编撰之初就要考虑现存国际法规则是否适用网络空间这个前置问题[2]17。鉴于国际社会没有一项明确的国际法规则治理国际网络空间,要创制新的统一国际法规则,困难是非常大的。手册的起草者们采取的办法是将现有国际法规则“投射”到国际网络安全中。为增强说服力,起草者们引用了大量的国际公约、公法学家学说或学术成果、国际法院的判例和相关国家的政府文件。《塔林手册》共计7个章节95条规则,每一条规则都有起草者的评注,评注通常对规则的目的、缘由和适用做解释。③

目前,《塔林手册》未达到一般国际法的高度。第一,《塔林手册》不是国际条约。手册的制定者是CCDCE的专家学者。该中心由北约7国④通过签署协议的方式于2008年成立,目的是提高北约的网络防御能力并制定相关网络防御准则⑤。虽然中心有主权国家的参与,但手册的制定者不是国家,而是47位来自法律界、技术界等领域的专家,手册制定后也未得到成员国的追认或签署。第二,《塔林手册》远未达到习惯国际法的高度。一项规则要成为习惯国际法规则,必须要满足两个要素:国家实践和法律确信。虽然《塔林手册》将业已确立的部分习惯国际法规则,比如禁止武力使用等规则纳入其中,但仅通过纳入是不能同时赋予国际网络规制习惯国际法规范的。另外,各国既未在国家实践中通过直接或间接的方法按照手册规则行事,也没有认为手册的内容体现了通行的国际规范。实际上手册起草者们也承认:“手册不是一个官方文件……手册甚至不代表北约网络防卫中心和北约组织的观点;手册也不反映北约处理网络安全的态度。”[2]23

《塔林手册》是一部无法律约束力的文件,它只是CCDCE的研究成果而已。但值得注意的是,随着CCDCE成员国呈逐步扩大的趋势以及国际社会对网络安全规制的要求深入,《塔林手册》以后是否会成为国际网络安全的示范法(model law),手册会不会得到北约各成员国的承认,得到肯定答复的可能性也绝非没有。

二、《塔林手册》中对“武力使用”的认定

禁止使用武力是《联合国宪章》第2条第4项规定的。该原则受到广泛讨论,但直至今日对“武力使用”仍结论不一。《塔林手册》第2章阐述了网络中的“武力使用”。手册第10条认为对他国进行网络攻击是违反国际法的;第11条界定了网络中“武力使用”概念;第12条认为国际网络环境中的“威胁武力使用”也是不符合国际法的。手册试图从两个方面说明网络攻击属于国际法上的“武力使用”:第一,区分武力使用和干涉的网络攻击行为;第二,要认定国际网络攻击属于国际法上的“武力”需要考虑到攻击的“规模”(scale)和“效果”(effect)这两大要素。

(一)区分国际法上武力使用和干涉的网络攻击行为

《塔林手册》第10条及评注将不同的网络攻击行为分别认定为国际法上的武力使用和干涉行为。手册第10条认为,对他国进行网络攻击构成对他国领土完整或政治独立的破坏,网络攻击行为和联合国目的不符因而是不法的。该条第4项评注为:“非一国的武装力量实施的网络攻击行为也构成武力使用。若网络攻击由一国情报机构或攻击行为可归功于一国的私人行为者实施的,该网络攻击构成国际法上的武力使用是明确的。”[2]46手册将网络攻击行为定性为侵犯主权的行为。手册将武装力量实施的网络攻击认定为武力使用,但对于私主体、组织团体和恐怖组织等非国家行为体实施的网络攻击却不认定为武力使用行为。

《塔林手册》第10条及第7至10条评注将未达到武力使用阶段的网络攻击行为定性为国际法的干涉(intervention)。手册认为网络攻击行为可能违反了这一原则,但对于何种程度的网络攻击为干涉,手册没有回答实际上也没法回答。评注第8至10条同时认为要区分网络干扰和网络干涉这两个概念,比如网络干涉一定要有强迫性(coercion),仅采取网络侵入,如攻破网络“防火墙”或密码等行为不足以构成网络干涉。若网络攻击达到改变一国

选举结果、散布错误消息等进而改变一国政体的话，该网络攻击就构成了“干涉”。

（二）界定构成武力使用的网络攻击行为的两大要素

《塔林手册》第11条从“规模”和“效果”两个要素认定构成网络攻击中的“武力使用”。手册从八个方面界定了构成武力使用的特征：严重性（severity）、即时行（immediacy）、直接性（directness）、入侵性（invasiveness）、影响的可测性（measurability of effects）、军事性（military character）、国家参与（state involvement）和合法性假设（presumptive legality）。

手册援引了国际法院1986年“尼加拉瓜诉美国”一案，并误认为法院在该案确认了“规模”和“效果”是区分武力使用和非武力使用的两个要素。其中规模要素为网络攻击的数量，影响要素为网络攻击的程度大小。[2]47手册并没有回答多少数量和多大程度的网络攻击属于武力使用。 第11条第2项评注也认为没有一个权威的概念来界定武力使用的准则。但手册并没有放弃对网络攻击中的武力使用给出一个明确的答案，并认为导致人员死亡、目标毁坏的网络攻击行为属于国际法上的武力使用。按照《塔林手册》对构成武力使用的网络攻击划分的八项标准，属于规模要素的标准为“严重性”和“影响的可测性”，其余六项标准属于效果要素。

1. 规模要素

《塔林手册》对认定何种网络攻击为武力使用的规模要素，理由比较薄弱。规模要素通常要考虑到攻击影响的范围、受攻击对象的多寡、损失大小等要素。手册认为导致个人生命、财产损害或国家利益受损的网络攻击行为均可被认定为武力使用。针对网络攻击的虚拟性特征，手册还通过非穷尽列举的方式将一定规模的网络攻击行为，比如根据受损数据的数量、瘫痪的服务器数量、被泄漏的机密文件的数量等作为认定构成武力使用的规模要素。手册认为之所以将规模要素考虑其中，原因在于考察网络攻击的数量等规模要素比较容易。但实际情况是，每日发生的数以亿计的大大小小的网络攻击行为，甄别单个网络攻击主体的具体数量和规模是困难的，并且现在的计算机反网络攻击技术远未发达到这种地步，这也是手册没有办法解决的技术问题。

2. 效果要素

效果要素是个颇具弹性且无统一内容的价值判断标准。《塔林手册》认为网络攻击具备即时性、直接性、入侵性、军事性、国家参与和合法性假设这六点效果要素，可以被认定为武力使用。即时性指网络攻击造成的影响是即刻的，只有构成即刻影响的攻击行为才是武力使用；手册对到底什么时间为即刻没有明确规定，但认为超过数周或数月才受到影响不属于武力使用。直接性是指网络攻击行为与受损结果存在直接的因果联系，手册认为存在直接的因果关系连接点是明确网络攻击主体和是否存在武力使用的重要一环。入侵性是网络攻击本身的特征，实际上网络攻击本身就暗含了入侵的特征，否则无攻击可言；但视网络攻击为武力使用，其入侵性的性质很显然要高于一般网络攻击。手册认为网络攻击发生在另一国境内且攻击的对象必须和一国国家利益有关，比如相比一国大学或商业机构的网络而言，入侵一国的军事网络就属于使用武力。很显然，手册暗含这样一种观点：构成武力使用的网络攻击行为，攻击对象应该是国家政治、军事等具备高阶化的政治军事组织；另外，手册将网络间谍排除出使用武力的范畴，并认为国际法并没有将网络间谍视为国际不法行为。网络攻击的军事属性是《塔林手册》一直强调且构成武力使用的重要要素，手册承认《联合国宪章》第2条第4项所指的武力是指军事力量，因此军事力量发起的网络攻击实际上属于武力使用问题。同样，手册将国家参与网络攻击看成是武力使用，即网络攻击的国家参与性。对于合法性假设这点，手册的阐述是相当模糊的。手册引用国际常设法院在1927年“荷花号案”确立的“国际法不禁止即自由”原则⑥，因此在认定某种网络攻击是否构成武力使用要通盘考察现行国际法规则，若国际社会没有存在一项规则认定某种网络活动是违反国际法的，那么该网络活动是符合国际法的[2]52。

三、对《塔林手册》认定武力使用的评析

《联合国宪章》第2条第4项规定了禁止国家使用武力或进行武力威胁。《塔林手册》借助宪章对武力使用的禁止性规定，认为网络攻击，特别由军事机构或国家参与的针对他国军事或国家利益的网络攻击属于国际法上的武力使用。手册主要从两个维度认定网络攻击属于武力使用：第一，应对武力使用中的“武力”采取扩大解释，即网络攻击属于武力使用；第二，满足“规模要素”和“效果要素”的

网络攻击属于武力使用的范畴。笔者认为,《塔林手册》扩大解释武力使用是与《联合国宪章》本意不符的;《塔林手册》认定的"规模"和"效果"两大要素的立论基础也是错误的。

(一)网络攻击不属于《联合国宪章》所指的武力使用范围

"武力使用"的解释是《联合国宪章》第2条第4项一个特别有争议的问题。对于"武力"一词的解释分为两个截然不同的观点⑦:第一种观点认为应对"武力"一词做狭义解释,即仅包括武装或军事力量;第二种观点认为应对"武力"一词采取扩大解释,即不仅包括武装或军事力量,还包括非武装力量的强迫形式。本文认为,应对宪章中的"武力"一词做狭义解释。众所周知,《联合国宪章》是一项最普遍的国际间条约,对宪章本身的解释应遵守1969年《维也纳条约法公约》中的条约解释通则。按照条约解释通则,条约解释有约文解释(文本解释)、整体解释(上下文解释)、目的解释(立法目的解释)和善意解释这四种解释方法。其中条约解释应以约文解释优先,其余的三种解释方法可以参照使用。如果条约的用语仍然不明确的话,应参考包括条约的准备工作及缔约情况的相关资料做辅助解释。首先,文本含义上的"武力"一词指"武装力量",即军事部队所使用的力量;其次,按照旧金山会议有关《联合国宪章》的准备会议工作文件,在起草宪章第2条第4项的过程中,军事力量之外的胁迫就被排除在"武力使用"一词之外;再次,参照《联合国宪章》第44条关于安理会决定动武规则将"武力"一词限定为军事力量以及第51条关于自卫权中有关军事力量反击军事力量的规定,均表明了宪章所指的"武力"为军事力量,宪章并无意图扩大"武力"一词的含义;最后,从联合国实践及司法实践来看,联合国不承认军事之外的力量比如经济和政治胁迫为"武力使用",国际法院在1986年"尼加拉瓜诉美国案"对"武力"一词也持狭义解释的主张⑧。

《塔林手册》对"武力使用"一词持扩张的解释,其理由有三点[2]45、48:第一,1970年《国际法原则宣言》规定了对国家采取一切包括经济胁迫在内的力量都是违反领土或政治主权的,网络攻击显然应该被包括其中;第二,国际法院在"核武器咨询意见案"中第39段对"武力"持扩张解释的观点;第三,国家实践已经开始主张网络攻击属于武力使用范畴。《塔林手册》提出的这三点理由值得怀疑。1970年《国际法原则宣言》一般被认为是对《联合国宪章》基本原则的解释文件。1970年宣言确实在序言第9段规定:"各国有义务在国际关系上避免……使用军事、政治、经济或任何形式的胁迫。"但结合宣言第3项原则——"不干涉内政原则"中禁止任何国家使用或鼓励使用经济等任何措施强迫国家的规定便得知,宣言第9段和不干涉内政原则相关联。实际上负责宣言起草的委员会在讨论禁止武力使用的过程中对"武力"一词进行了讨论,最后一致认为,"武力"不包括经济胁迫并留给不干涉原则调整⑨。至于《塔林手册》提出的有关国际法院1996年"核武器咨询案"中对"武力使用"采取的扩张解释观点,笔者认为,手册在没有通盘考虑咨询案的整体情况下便做出断章取义的主张是不适当的。该案实为国际法院认定核武器是否为国际法禁止的武器范围,即核武器是否可以成为武力使用的一种手段。法院虽然认为《联合国宪章》既不明确禁止也不明确允许使用包括核武器在内的任何具体的武器,但这不等同于法院已对"武力"一词做扩张的解释。恰恰相反的是,法院也认为:"这种禁止使用武力的规定应根据宪章其他的有关条款来看……"⑩实际上法院及其审案法官对核武器是否是武力使用且是否合法的认识也是含糊不清。正如时任院长贝贾维指出:"国际法院仍得不到判定,按照国际法的现状,很不幸,它无法对这个问题做出明确的答复。"⑪至于手册提到已开始有国家实践认为网络攻击属于武力使用,这样的观点更是毫无根据的。目前为止,没有任何国家通过实践表明网络攻击属于武力使用的范畴。《塔林手册》将网络攻击纳入国际法上的"武力使用"范围是不符合宪章本意和国际法发展现实的。

(二)"规模"和"效果"两大要素的立论基础错误

《塔林手册》并没有不分青红皂白地将一切网络攻击视为国际法上的武力使用,而是采取要素理论确立其立论的基础。为了使立论更具说服力,手册引用国际法院1986年"尼加拉瓜诉美国案"并认为国际司法实践确立了"规模"和"效果"是构成武力使用的两大要素。但手册的起草者们对该案的理解是偏颇的。实际上国际法院是在这样一种语境下对"规模"和"效果"进行论证的,即一国派遣武

装团伙到另一国境内的行为因“规模”和“效果”等同正规军实施的武装攻击，可以被列入武装攻击的范围内[12]。很显然，国际法院并没有认为“规模”和“效果”是构成武力使用的两大要素，而是在同为武装力量性质前提下将同样规模和效果的武装团伙力量也纳入到武装攻击的范畴之内。另外，法院更没有将这两大要素推广至认定某种攻击行为是否为武力使用的意图。除了手册认定的两大要素的立论前提错误外，手册对要素涵盖标准的论证也是令人怀疑的。比如手册主张的“合法性假设”标准同样误读了1927年国际常设法院“荷花号案”的判决。“荷花号案”中法院提出的“国际法不禁止即自由”主张是一国处理内部事务、解决内部规则应遵循的。也就说，除非国际法有禁止性规定，否则一国在其领土管辖范围内自由处理内外事务[13]。“荷花号案”确立的原则只适用于国家处理内部事务，而不适用处理国家外部事务和管辖权分界问题。国际网络攻击的产生和结果不可能都在一国境内发生，其将来的法律规则必然涉及到国家间网络管辖权和外部事务。《塔林手册》将“荷花号”原则适用至国际网络行为规制当中是对国际司法实践的误读。

除此之外，手册对网络攻击在什么情况下构成国际法上的武力使用的规定是不明确的。比如手册认为由军事力量和国家实施的对另一国的网络攻击并造成国家利益或人员或财产损害的，应构成武力使用，此种情况的发生究竟是在平时状态还是战争状态：如果是发生在国与国的战争状态，那么网络攻击充其量是一种作战方法而已；但攻击如果发生在平时状态，到底多大程度的网络攻击方法和手段构成武力使用，这些问题手册并没有解答。另外，由于网络攻击本身隐蔽性强，攻击者身份不易识别，如何确认行为和结果的直接因果联系，在法律上是值得怀疑的。最后，手册对武力使用和网络攻击规范的连接显得比较粗浅，其中的绝大多数规则是移植性的而非在科学论证的前提下进行的法律创制，这使得《塔林手册》在国际法上的说服力大打折扣。

四、武力使用规则与网络战争之国际法反思

武力使用是国际法常且新的话题。谓之“常”是因为在国际法学科诞生之初，武力使用和战争这一对“孪生兄弟”就出现在国际社会的话语体系之中。谈其“新”乃是现代科技迅速发展带来的武器或作战手段问题迫使国际法做出不断的新回应。比如针对核武器产生的问题，国际法院先后在1974年“核试验案”、1996年“一国在武装冲突中使用核武器的合法性问题咨询案”和“以核武器相威胁或使用核武器的合法性咨询案”中做出判决或咨询意见。从法院在这三起案件中由先前的模糊到之后较为明确的态度可知：国际法规则和国际社会现实处于一种彼此分离又交相互动的复杂关系。彼此分离并非国际法不愿调整新问题，而是国际法和国内法一样本身具有规则调整的滞后性；彼此互动不仅源于国际法本身规则的张力特性，也囿于国际法不可能超然国际关系现实之外，国际法要有生存和发展的“土壤”必然要对国际社会现实做出回应，而这种回应的过程必然有不断持续的互动关系，而且这种互动显然不会一帆风顺。

一直以来，网络安全属于一国主权管辖的事项。但随着近十年来针对国家安全的网络攻击不断出现，网络等非传统安全备受关注。国际网络安全并非仅通过技术方面的反打击就可以解决，恰恰相反的是，国际社会更需要一种较普遍的国际规则来对网络安全进行规制。虽然《塔林手册》对“武力使用”的论证有诸多法理的缺陷，但是手册试图对现存国际法规范所做的移植以及探寻国际规则的努力是有价值的，其价值在于反思国际法规则是否可以进行动态解释。

如前文所述，按照条约解释的通则以及实证国际法的态度，武力使用显然应该做狭义解释[14]。按照狭义解释，《塔林手册》所持的将“网络攻击”视为武力使用的范畴是不恰当的。但是对“武力”一味地坚持采取约文等严格的解释方法，会导致法律规则无法对实际问题做出回应。况且采取约文等解释办法本身较为适合规则简单明晰的情况。纯粹法学派学者汉斯·凯尔森（Hans Kelsen）在《国际法研究：国际法的集体安全》一文中就认为《联合国宪章》中的“武力使用”既包括使用武器，也包括在一国境内行使权力但不适用武器的违反国际法的行为[3]。对“武力”一词采取狭义和扩大的两种解释方法反映了国际社会不同的价值主张。扩大解释方法是一种动态的解释方法，该方法可以实时反映国际关系的新发展。但是对“武力”采取无限制的动态解释一方面破坏了规则的相对稳定

性,另一方面会强化国际法的“权力规则”色彩,而这对国际法的稳定性结构是不利的。本文认为,对“武力”一词解释不应做不周延的且不合理的扩大解释。以网络攻击为例,不是所有的网络攻击都不能被解释为“武力”,而是不能被笼统且划一解释为“武力”。只有那些针对国防、军事设施实施的网络攻击才可以被认定为“武力使用”⑮。另外,随着网络安全规则的不断形成和发展,联合国等国际组织的相关实践可以为“武力”提供新的解释内容,或者由联大或安理会请求国际法院对网络攻击是否构成“武力”发表咨询意见也是一种可能的办法。

五、结　语

网络安全和网络战争是最近几年国际社会普遍讨论的议题。随着各国网络军事化的开展,网络安全、网络攻击和网络战争等话题必然在国际社会得到进一步关注。作为国际上第一部系统论述网络安全、网络攻击和网络战争的文件——《塔林手册》并未具备一般国际法的高度,手册本身也不是一种法律创制。手册的起草者为北约研究中心的独立专家团,迄今为止手册所载的规则也未得到有关国家的承认;另外,手册的规则是对既有国际法规范的移植,并没有创造出一套新的适用于国际网络攻击和国际网络战争的规则。

手册对网络武力使用的认定关系到行使网络自卫权等一系列国际法理论和实践的前置议题,何种网络攻击构成武力使用是必须要仔细考查的问题。单从国际法论据的正当性和合法性上看,手册对宪章中“武力使用”一词持扩大解释以及曲解国际司法实践的做法是站不住脚的。因为按照条约解释规则,“武力使用”应被严格解释为军事力量的使用;另外,任何一项主张或诉求要通过国际司法实践进行佐证,不能通过断章取义和任意扩大司法机构意图的做法来“粉饰”表面的正当性和合法性特征;从国际法的整体性上看,手册对“武力使用”持扩大解释的方法也反映了国际法规则本身的张力特性。扩张解释和严格解释这两种法律解释方法本身也反映了国际社会不同价值主张的路径,这两种路径的任何一种并非永远处于上风和优势地位,这需要国际法学者和实践者在国际法和国际社会的发展现实的背景下择取一种路径去主张。本文认为,目前将网络攻击认定为“武力使用”的主张既不符合国际法规则,也不符合国际法和国际社会的发展现实。网络攻击中武力使用问题是属于国际法的传统问题。尽管《塔林手册》认定网络武力使用的法律论点和论据存在诸多法理缺陷和实践误读,但其表达的国际法主张是不能被忽略的。随着北约卓越合作网络防卫中心目前的成员国数量不断增加,手册所持的国际法诉求不可能一直停留在学理主张层面。中国作为互联网的使用大国,也是互联网受攻击严重的国家,需要在国际网络规制话语体系中体现自己的主张。《塔林手册》涉及的国际法律问题值得中国国际法学界深入研究和回应。

注释:

① 中方的立场请参见“外交部就中美网络安全的回答”,网址:http://news.xinhuanet.com/world/2013-03/14/c_124460398.htm,访问日期:2015年12月3日。

② 比如2007年发生在北约同盟国爱沙尼亚、2008年格鲁吉亚和俄罗斯战争期间、2010年伊朗以及2014年乌克兰的网络攻击事件。

③ 有关《塔林手册》的述评,可参见Terence Check,“Book Review: Analyzing the Effectiveness of the Tallinn Manual's jus ad bellum Doctrine on Cyber Conflict, A NATO-Centric Approach”,载Cleveland State Law Review,2015,63(2),495-513页;陈颀:《网络安全、网络战争与国际法——从《塔林手册》切入》,载《政治与法律》,2014年第7期。

④ 这7个国家分别为爱沙尼亚、德国、意大利、西班牙、斯洛伐克、立陶宛和拉脱维亚。

⑤ 除北约7国外,美国以观察员身份参与,防卫中心接受非北约国家加入;2014年5月30日,捷克共和国、法国和英国成为中心成员;2015年7月1日瑞典加入防卫中心。截至2015年9月4日,防卫中心共有14个成员国和1个观察员国。

⑥ 实际上《塔林手册》对1927年“荷花号案”的解读是错误的,本文将在第三部分的评析中对此误读做出回应。

⑦ 有关《联合国宪章》第2条第4项条款的解释讨论,请参见黄瑶:《论禁止使用武力原则——联合国宪章第二条第四项法理分析》,北京大学出版社2003年版,第167页—第177页。

⑧ 参见Case Concerning the Military and Paramilitary Activities in and Against Nicaragua(Nicaragua v. United States of America),ICT Report,1986年,第101页第191节。

⑨ 参见UN Doc. A/AC.125/L.16;L.21,1970。

⑩ Nuclear Weapons Advisory Opinion, para.38。

⑪ Nuclear Weapons Advisory Opinion Case, ICJ Reports, 第110页。

⑫ Nicaragua Judgment, 第195节。

⑬ Lotus Case, 18-19页。有关“荷花号案”的论文参见陈一峰:《国际法不禁止即为允许吗?——“荷花号”原则的当代国际法反思》,载《环球法律评论》2011年第3期,第132-141页。

⑭ 本文对《塔林手册》的论点所做的批判是持实证主义态度的,本部分的叙述并非和文中观点相左而是笔者对国际法发展现状的一种反思。

⑮ 《塔林手册》将对平民和国家的网络攻击都看成是“武力使用”的范畴,这是本文无法认同的。本文前文对此有阐述。

参考文献:

[1] M N Schmitt .Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework [J]. Research Publication 1 Information Series, 1999 (June).

[2] M N Schmitt .Tallinn Manual on the International Law Applicable to Cyber Warfare[M]. Cambridge: Cambridge University Press , 2013.

[3] Hans Kelsen. International Law Studies: Collective Security under International Law: vol.49 [M]. U.S. Naval College, 1957.

责任编辑:刘伊念

(Email:lynsy@jhun.edu.cn)

Use of Force in the Cyber Warfare as Defined in Tallinn Manual

——Analysis from the Angle of the International Law

JI Hua

(School of Law, Peking University, Beijing, 100871)

Abstract: Refraining from the use of force is specified in Item 4, Article 2 of The Charter of the United Nations and is also a rule of jus cogens. Although The Charter of the United Nations does not define “the use of force”, the word “force” should be restricted to the military category according to the rules that are used to interpret treaties. As a document intended to regulate international cyber security, however, the Tallinn Manual qualifies cyber-attacks as “use of force”. The Manual is neither legally binding nor is a legal creation; the qualification of the use of force in the Manual is both defective in theory and misleading in practice. The Tallinn Manual's definition needs to be responded to and reconsidered by traditional rules of the international law.

Key words: cyber security; cyber warfare; international law; Tallinn Manual; use of force; The Charter of the United Nations