网络攻击中国家自卫权行使的国际法思考

石　榴

（宁夏大学新华学院）

摘　要：随着网络信息技术的发展，网络攻击成为影响国家安全的一个很大隐患。国际社会中出现大规模的网络攻击事件，对各国造成了严重损失，因此其有关问题便成为国际社会关注的重点，针对网络攻击的相关国际法规制，各主权国家尚未形成统一共识，对于《塔林手册》如何适用也持有不同观点。越来越多的国家面临日益复杂多变的网络安全威胁，因而维护网络安全合乎各国的共同利益，各网络大国应首先达成网络安全相关问题的共识，从网络攻击中国家自卫权行使的角度出发，分析主权国家面对网络攻击如何行使自卫权出现的问题，探讨这些问题应如何解决与完善，从而维护国际社会网络安全的和平与稳定。

关键词：网络攻击；自卫权；网络主权；网络空间

International Law Thinking on the Exercise of National Self Defense Rights in Cyber Attacks

Pomegranate

（**Xinhua College of Ningxia University**）

Abstract: With the development of network information technology, network attacks have become a major threat to national security. The emergence of large-scale cyber attacks in the international community has caused serious losses to countries, so its related issues have become the focus of international attention. Sovereign countries have not yet formed a unified consensus on the relevant international law regulations for cyber attacks, and they also hold different views on how to apply the Tallinn Manual. More and more countries are facing increasingly complex and volatile cyber security threats, so maintaining cyber security is in the common interest of all countries. Major cyber powers should first reach a consensus on issues related to cyber security. From the perspective of the exercise of the right of self-defence by cyber attack countries, this paper analyzes the issues that arise when the dominant countries exercise their right of self-defence in the face of cyber attacks, and discusses how these issues should be resolved and improved, Thereby maintaining the peace and stability of the international community's cybersecurity.

Key words: network attack; The right to self-defence; Network sovereignty; Cyberspace

2022 年 6 月 22 日，西北工业大学邮件系统遭受境外网络攻击，黑客组织和不法分子发送包含木马程序的钓鱼软件，部分教职工的个人电脑中发现遭受网络攻击的痕迹。经调查确定此次西北工业大学遭受的网络攻击系美国国家安全局（NSA）下属“特定入侵行动办公室”及其雇员所为。

国家计算机病毒应急处理中心报告显示，在近几年里，美国国家安全局下属 TAO 对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备，窃取了超过 140GB 的高价值数据，并且在攻击过程中，TAO 会根据目标环境对同一款网络武器进行灵活配置。

有鉴于此，在网络安全问题日益严峻的今天，对于网络攻击进行国际法规制成为必须面对和思考的重大问题。国际社会也亟须发挥国际法对网络空间命运共同体的保障性作用，而广泛的国际共识将成为统领一切之核心。

一、网络攻击中国家行使自卫权概述

（一）网络攻击的基本概念

近些年来，网络攻击事件一直持续发生，在信息网络发达的大背景下，网络攻击已经成为一种新型攻击方式，更是被上升到网络战争的高度。但现阶段的国际社会并未就网络攻击的概念达成一致意见，实践中往往出现“网络攻击”一词被滥用的情况。《塔林手册》是北约卓越合作网络防御中心制定的网络战规则，对国际社会中的网络攻击具有很重要的参考价值，相应的，其对于网络攻击的定义也被业界所认可。《塔林手册 2.0》里将网络攻击定义为：“无论进攻还是防御，网络攻击是可合理预见的会导致人员伤亡或物体损毁的网络行动。”[1]

（二）自卫权的基本概念

在国际法上，自卫权被认为是主权国家天然所具有的自然权利，因为一旦国家遭遇武装攻击，便有权使用武力手段抵抗外来侵略。根据《联合国宪章》第 51 条规定，国家有单独或集体进行自卫的权利。[2] 根据《联合国宪章》第 2（4）条规定，国家是禁止使用武力或武力威胁的。但为了防止受害国在遭受武力攻击时因为没法开展行之有效的救济从而造成难以弥补的损失，《宪章》第 51 条对禁用武力这条原则作了除外要求，即国家在遭受武力攻击时，有权使用武力进行自卫从而维护国家主权及其人民的生存安全。

（三）网络攻击的特征

1. 网络攻击具有隐秘性

传统的武装攻击发生在现实空间，而网络空间是一种非实体的虚拟空间，所以其攻击场所难以确定，不像现实所见的传统武装攻击在陆地、深海、高空等地方具有实际的边界，而网络攻击没有现实的战斗地区，攻击场所为虚拟网络空间。还存在着网络攻击者利用自身精湛的互联网技术，转移视线销毁痕迹溜之大吉的问题，很难找到实施者和证据。

2. 网络攻击的“武器”具有特殊性

冷兵器时代的武装攻击大都使用刀，箭，棍，鞭，叉等；自一战、

二战进入热战以来，武器发生了质的变化，武装攻击大都是通过枪、炮、导弹等热武器对别国发动战争；而进入到信息技术时代以后，网络攻击则成为了一种新的攻击手段，具有信息技术性，通常采取植入计算机病毒、组织利用黑客等破坏、篡改他国重要的电子计算机存储数据，窃取他国军事或政治机密、重要数据，威胁国家网络主权，造成重大国家损失。

3. 网络攻击具有连续性

实施网络攻击一般都是利用计算机等网络设备，只要在手头有设备，有电源就可以连续不停、不分昼夜的进行密集的攻击，乘虚而入，使得受害国来不及及时反应，因而发动网络攻击具有来无影去无踪的特点，可以在短时间内迅速结束，而损失则往往是毁灭性的。

二、国家行使网络空间自卫权的具体条件

（一）实质条件

1. 行使网络空间自卫权的对象

从《联合国宪章》第 2 条第 4 款规定可见[3]，行使自卫权的对象通常是指主权国家。但根据《联合国宪章》第 51 条的规定，一国行使自卫权的先决条件仅限于使用武力进行攻击，行使自卫权的对象主要是国家但不局限于国家，在某些情况下，非国家行为主体也可能成为国家行使自卫权的对象。根据《联合国宪章》的规定，一般情况下，国家无法对纯个人，无政治团体操纵实施的网络攻击行为行使自卫权，除非个人行为归因于国家，这就要求特别注意眼前的网络攻击是纯黑客个人行为，还是由政府或者军方蓄意操纵，并为其服务。如果受害国掌握了足够的证据，能够证明黑客或者个人在政府或军方的掩护或支持下对其他国家进行网络攻击行为，则可以成为国家行使网络空间自卫权的对象。

2. 必要性原则和相称性原则

根据国际法相关规定，面对武装攻击时，国家的自卫行动必须严格遵守必要性和相称性原则。

必要性原则是指；受攻击的国家处于紧急态势，如不采取武力反击，自己本国的主权安全和领土完整将会遭受巨大损害，必须是在没有其他切实可行的和平手段可供选择作出反应的情况下，这个时候的自卫权行使才是必要的，才能使用武力。在当今的国际社会我们强调减少冲突，争取协商沟通，和平对话，斡旋或者调停，诉讼或者仲裁等和平方式来解决国际争端。“相称性”又称“成比例性”或“程度相当原则”，要求国家在行使自卫权时，其所使用的武力程度与所遭受的损害之间，所保护的权益与可能造成的损害之间必须具有一个适当的度。[4] 比如甲国武力侵犯乙国边境，乙国可以采取自卫行动，击退甲国撤出乙国即可，而不能直接使用核武器使讲消失在地球，这样就违背了相称性，自卫反击手段超过了度。那么，一国在遭受网络攻击中，为维护本国网络安全，国家主权，行使自卫权而采取的手段、保护的利益以及所造成的损害都须是相称的。[5]

时间来到 2011 年 6 月 4 日那天，美国前国防部长盖茨来到新加坡，这一行程内容和网络攻击有关，参与亚洲安全会议，并在会议上发表讲话，第一次清楚地表明当发现本国如若遭到其他国家的网络攻击时，将“视之为战争行为并予以武力还击”。[6] 但即便如此，由于网络攻击具有巨大的破坏性和难以预测的危险性，这种做法也要受到必要性和相称性原则的限制。

（二）程序条件

1. 国家行使网络空间自卫权的时间

现如今，攻击或侵略他国不仅仅发生在现实空间“海陆空”之中，进入信息化时代，攻击手段也越发具有技术性，隐秘性，科技化，网络空间也成为了新的战场，因而有必要对网络空间的主权安全实施保障，进行国际法规制。根据《联合国宪章》第 51 条的规定国家行使自卫权的前提条件必须是“受武力攻击”，在安理会采取维护国际和平与安全所采取的必要措施之前，即一旦安理会采取了维护国际和平与安全的必要措施，自卫行动即告结束，《塔林手册 2.0 版》规定，“当网络武力攻击已经发生或迫近时，可使用武力行使自卫权。自卫还要遵循迅即性的要求。”[7]

针对网络攻击从而行使自卫权现实中还没有被实践过，安理会也没有对网络攻击采取过具体行动。因而，针对网络攻击，能不能、如何行使自卫权基本都处于理论阶段。

2. 向安理会报告的义务

国家行使自卫权必须向安理会报告在《联合国宪章》里面有明文规定，在《塔林手册》规则 17 中也规定“根据《联合国宪章》第 51 条，行使自卫权时，各国进行网络军事行动涉及的措施应及时向联合国安理会报告”。[8] 国家如果决定要行使国家自卫权，国家不仅要及时报告，而且还需向安理会提供关于遭受武力攻击的事实、采取自卫权的必要性、相称性等方面充分的证明材料，以供安理会准确及时的下决定。但现实的情况是，受害国它们觉得没有必要报告，因为自卫权是国家本身的一项自然权利，可以自己决定。

三、中国应对网络攻击的对策

（一）合法行使自卫权

一般来说，面对网络攻击，如若受害国想行使自卫权，那么网络攻击的破坏性应足以达到武装攻击的程度，其破坏程度应该是巨大的，也就是说该网络攻击行为对被攻击国家造成国家机密泄露，国家网络主权遭受威胁或重大财产损失。根据《联合国宪章》第 51 条的规定，行使自卫权的先决条件是是一国遭受到另一国的“武力攻击”。网络攻击如果构成该条所指的“武力攻击”，那么，受害国能援引宪章这一规定行使自卫权吗？《联合国宪章》并没有明确定义，根据国际法院关于“尼加拉瓜案”[9] 事件的判决，所有的武力攻击都属于使用武力，但并非所有使用武力都构成武力攻击，只有最严重、最具破坏性和最具有显著规模的使用武力才能构成“武力攻击”。因而，有关的国际立法应明确规定，网络攻击的受害国是否可以利用网络或武装部队来打击网络攻击。此外，应当指出受害国必须根据攻击的类型和损害的程度采取适当的自卫措施，要符合“必要性”和“相称性”要求。而且要由联合国安理会决定能否使用自卫权对实施侵略、破坏和平、威胁和平的国家所发动的网络攻击进行规制和惩罚。

（二）积极参与国际立法工作

在目前的网络安全立法中，大多都是发达国家的立法规则和条款，它们凭借自己掌握的网络科学核心技术，通过立法来保障自己的各方面利益。我国作为最大的发展中国家，世界第二个经济体，全球网民数量最多的国家，应联合其他国家或国际组织，积极参与国际立法，遏制少数国家的网络霸权，争取营造一个和平的网络世界环境。

此外，为规制他国利用网络进行国家攻击的行为，以本国利益为基础，维护国内国际网络空间主权安全，我国需提高国际话语权，把握主动权，因而要加大网络空间相关各领域人才的培养。以《塔林手册》的编订为例，我国仅有一位专家参与，这不能不令人反思。有鉴于此，我国应加快培养具有网络安全技术、国际关系和国际法等领域的高级人才，这样的话，便可以为我国将来参与网络空间国际规则的制定储备各方面专业人才。要有法治信仰、中国立场、国

际视野和平民情怀。

（三）积极提倡发挥联合国安理会的职能

当发生网络攻击时，安理会有权判断网络攻击是否构成对和平之威胁，和平之破坏，抑或是否为侵略行为，并在《联合国宪章》第 41 条或第 42 条框架下通过相关决议，可分别授权会员国采取非军事或军事行动。但是，网络攻击是不是武力攻击？能否把网络攻击划归为武力攻击、至今没有形成共识，仍存在很大争议，应先由联合国安理会做出判断，因为安理会有承担维护国际和平与安全的职权。在此理论基础下，可以由联合国安理会通过相关决议，授权采取实际行动，使受害国的权益得到救济；同样，这也表示，如果安理会没有通过决议，受害国为了维护本国的国家安全，网络主权，最终可以诉诸必要与相称的自卫权。

中国是联合国的创始会员国之一，也是安理会常任理事国，积极参与联合国的各项事务活动。2020 年 9 月 18 日，中国发布《联合国成立 75 周年中国立场文件》，主张："安理会要发挥国际集体安全机制作用，承担维护国际和平与安全首要责任……中方坚决反对动辄使用武力或以武力相威胁……任何强制行动都应由安理会授权。"[10] 面对国家间日益繁多的网络攻击现象的发生，可不可以行使自卫权，如何行使自卫权等问题，各国还没有达成共识，为此，我们中国可以积极推动安理会在应对网络攻击事件时发挥建设性作用，在基于本国利益的立场上，中国也积极响应，为构建和平稳定的国际网络环境而努力。

（四）完善国内网络空间安全立法

我国不仅是世界上最大的发展中国家，也是全球网民数量最多的国家，因而为保障我国网络主权，信息网络系统稳定安全，必须建立完善有关网络攻击的国内法。现阶段我国缺乏具体解决国际间网络空间安全的相关法律法规，更没有针对网络攻击的法律规制。因此，我们可以通过组织国际法、网络安全、电子信息技术等领域的专家一起建言献策，群策群力，并在借鉴学习国际社会有关网络攻击先进立法经验的基础上，制定出符合我国利益的应对网络攻击的维护网络空间安全的法律体系。例如，在我国可以学习借鉴两版《塔林手册》，并根据我国实际情况，合理借鉴，同时创新思路，从而制定出科学合理的规范网络攻击的法律规则。在学习借鉴的过程当中，我们应该始终把我国的根本利益放在首位，充分考虑我国网络空间安全现状，争取网络空间的主动权，打赢信息战，网络战，维护我国的网络主权，并为共同促进国际网络空间的安全稳定而努力。

四、结语

如今，世界网络信息化，网络科学技术迅猛发展，国家间利用网络进行隐蔽性斗争越来越激烈，今后，网络攻击会愈加频繁。虽然各国纷纷开始重视此威胁，但关于网络空间领域尚未形成具有普遍约束力的国际法规则。《塔林手册》的适用具有局限性，也不能完全应对如今出现的各种问题。我们应研究分析现有关于网络攻击的国际法规则，着重从自卫权入手分析其适用的必要性和条件，从而达到合理规制网络空间自卫权行使的目的，避免自卫权的滥用，更好地维护世界的和平与安全。

参考文献

[1] 宋玉．网络攻击中的国家责任问题研究 [D]．河南：郑州大学，2021：22.

[2] 石梦杰．国际法视角下网络攻击的国家责任 [D]．上海：华东政法大学，2017：36.

[3] 张磊．论国家自卫权在网络攻击中的适用 [D]．北京：北京交通大学，2017：18.

[4] 黄志雄 .《塔林手册 2.0 版》影响与启示 [J]．中国信息安全，2018，(3)：85.

[5] 齐翰文．网络攻击国际法规制研究——以《塔林手册 2.0》为视角 [D]. 内蒙古：内蒙古大学，2020：6.

[6] 贺维．网络攻击的国际法规制研究 [D]．天津：天津师范大学，2019：25.

[7] 李淼．网络攻击国际法规制研究 [D]．黑龙江：黑龙江大学，2017：15.

[8] 李琦．网络攻击的国际法规制研究 [D]．辽宁：辽宁大学，2015：14.

[9] 王惠茹．和平时期下网络攻击的国家责任问题研究 [D]．吉林：吉林大学，2016：20.

[10] 金子煜．网络攻击国家责任认定问题研究 [D]．吉林：吉林大学，2022：19.

[11] 张华．论非国家行为体之网络攻击的国际法律责任问题——基于审慎原则的分析 [J]．法学评论，2019，(5)：160.

[12] 宋鹏．互联网攻击的国际法规制问题 [J]．法律制度建设，2021（2）：134.

[13] 朱莉欣．信息网络战的国际法问题研究 [J]．河北法学，2009，27（01）：51-53.

注释：

[1] 迈克尔·施密特 . 网络行动国际法塔林手册 2.0 版 [M]. 北京：社会科学文献出版社，2017：406.

[2]《联合国宪章》第 51 条："联合国任何会员国受到武力攻击时，在安全理事会采取必要办法，以维护国际和平及安全之前，本宪章不得认为禁止行使单独或集体自卫之自然权利。会员国因行使此项自卫权而采取之办法，应立向安全理事会报告，此项办法于任何方面不得影响该会按照本宪章随时采取其所认为必要行动之权责，以维护或恢复国际和平及安全。"

[3]《联合国宪章》第 2 条第 4 款："各会员国在其国际关系上不得使用武力或威胁，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。"

[4] 顾德欣：《战争法法律冲突》，载自《国际论坛》，2001 年 1 期，第 5 页。

[5] 辛柏春：《自卫权法律问题探析》，载自《学术交流》，2014 年第 9 期，第 84 页。

[6] 中国新闻网：《美国防长盖茨称将视网络攻击为战争行为》，2011 年 6 月 4 日，13：33。

[7]［美］迈克尔·施密特，［爱沙尼亚］丽斯·维芙尔：《网络行动国际法塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 351 页。

[8] Michael N. Schmitt Ed. Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, p. 64.

[9] 在该案中，国际法院对"最严重的使用武力"和"其他严重性相对较低的使用武力"进行了区分，认为一些措施"不构成武力攻击但涉及使用武力"。举例来说，一国向另一国叛乱组织提供武器和其他支持不属于对后者的"武力攻击"，但可能构成对禁止使用武力的违反。

[10]《中国关于联合国成立 75 周年立场文件》，外交部网站，http://new.fmprc.gov.cn/web/zyxw/W020200910425553975697. pdf。