网络战叙事的结构分析:主体和动因*

蔡翠红[1] 杰 古[2]

(1. 复旦大学美国研究中心 上海 200433;2. 复旦大学国际关系与公共事务学院 上海 200433)

摘 要 网络战过于宽泛的概念和它的任意使用引起了人们对于网络战叙事产生的背后原因以及其所声称的真实性的一系列猜测。从媒体报道、决策者和专家这三个主体角度分析了美国的网络战叙事,解释这个概念产生混淆的原因,并分析制造这些网络战叙事的主体表面的和潜在的利益动机所在。剖析这些利益主体及其不同动机能够对网络战研究有一定的启发,从而可以更加客观地认识网络战叙事并避免决策过程中的可能错误。

关键词 网络战 网络战叙事 网络威胁 网络安全 网络攻击 利益主体

中图分类号 D81 **文献标识码** A **文章编号** 1002-1965(2014)08-0025-06

DOI 10.3969/j.issn.1002-1965.2014.08.005

A Structural Analysis of the Narratives of Cyberwar: Subjects and Objectives

Cai Cuihong[1] Diego Dati[2]

(1. Center for American Studies, Fudan University, Shanghai 200433;
2. School of International Relations and Public Affairs, Fudan University, Shanghai 200433)

Abstract The concept of cyberwar has become too broad and its random use raises a series of doubts about the reasons behind the creation of such narratives and the genuineness of their claims. This article analyzes the narratives of cyberwar produced in the U.S. from the perspectives of media reports, decision makers and experts. It then explains why the concept has become so confusing and what are the explicit and concealed objectives of the actors producing such narratives. Dissecting these actors and their objectives will help to shed some light on the issue of cyberwar, in order to promote better judgment and avoid dangerous fallacies in the process of policymaking.

Key words cyberwar narratives of cyberwar cyber threat cyber security cyber attack actors

0 引言:网络战叙事

叙事(Narratives)通常是指我们对于一个故事的描述,即为了帮助我们处理复杂的现实,而将一系列事件通过一个结构更加合理和简洁的描述来加以解释和说明[1]。往往这些叙事就成为了不同利益主体的文字工具,一些事件和原因说明经过叙事的挑选和多次重复,可能就成为了"事实"。

网络战叙事(Narratives of Cyberwar)是在网络空间中以国家之间冲突为主题产生的故事。根据这些叙事的主张,网络空间已经成为一个战争域,在这个空间内,黑客们代表自己的政府或者支持恐怖组织破坏网络空间,引起相应的物理破坏乃至人员伤亡。"信息战"一词是指军方利用信息和通信技术来指导军事行动。由于"信息战"这个概念过于广泛,1993年,约翰·阿奎拉(John Arquilla)和戴维·龙菲尔德(David Ronfeldt)决定采用另外一个术语,即第一次兰德公司发表的"网络战来了!"("*Cyberwar is Coming!*")一文中的"网络战争"[2]。尽管作者承认使用这个新的概念需要进一步的说明,但是他们第一次描述它为"以干扰和破坏对方所依赖的信息和通信系统为目的的战争方式,这些信息广义地讲甚至包括军事文化"[3]。网络战争现在仍然是争论的主题,其范畴常常过于宽广而缺乏指导决策的意义。许多研究对它提供了不同的定义,但有的甚至根本没有提供定义,概念使用具有随意性。网络战缺乏明晰解释有很多原因,不同背景

收稿日期:2014-05-22 修回日期:2014-06-05

基金项目:国家社会科学基金项目"21世纪中美关系中的网络政治研究"(编号:12BGJ018);复旦大学科研项目"中美网络空间战略比较:差异、影响与中国应对"的成果之一。

作者简介:蔡翠红(1972-),女,博士,副教授,研究方向:网络政治、网络安全战略及中美关系等;杰 古(Diego Dati)(1983-),男,意大利籍,硕士研究生,研究方向:网络政治。

的人对之有不同的理解,换言之,不同的利益主体会有不同的网络战叙事。

为了分析方便,本文将产生网络战叙事的利益主体分成三大类:媒体、决策者和专家,然后进一步分析这些主体表面的和潜在的动机。剖析这些利益主体和他们的动机能够对网络战研究有一定的启发,从而可以更加客观地认识网络战叙事并避免决策过程中的可能错误。

1 不同主体视角下的网络战叙事

1.1 媒体报道中的网络战争:外来威胁、网络灾难与言过其实 媒体报道对于网络战争有许多不同的角度,但他们一般用三种叙事方式。第一种叙事是强调来自外来主体的威胁,例如美国对中俄网络威胁的渲染;第二种叙事关注于网络武器和网络灾难,例如臭名昭著的Stuxnet蠕虫病毒。这两种叙事往往会结合在一起并且搀和一些网络阴谋论和网络犯罪的故事,从而给读者呈现一幕充满怀疑味道的网络战叙事。第三种叙事,或许也是最不流行的,它声称网络战争还没有发生,并不像人们所说的会有那么严重的威胁。不同的叙事可能出现于同一媒体来源,因为这可使媒体避免明显的偏颇嫌疑。

网络战争自2007年开始成为媒体报道流行的题材。俄罗斯和爱沙尼亚之间的分歧引发了第一次世人熟知的网络战争。根据报道,俄罗斯黑客攻击了爱沙尼亚的网络,丑化了他们的政府官网,并引起一些服务不能正常使用。结果,爱沙尼亚政府和西方媒体开始推测俄罗斯政府参与了此次网络攻击。但截至今日,这起网络攻击是一次自发式民间黑客行为还是政府行为还不得而知。报道强调说网络攻击使爱沙尼亚失去了行动能力(paralyzed),但是真实情形并没有报道描述的那么严重。

当2008年俄罗斯和格鲁吉亚之间再次发生冲突时,媒体又谈论起网络战争。黑客在网络空间的行为与现实世界行动紧密相随似乎在网上网下之间建立了一个可能的联系,甚至有人怀疑俄罗斯政府和网络犯罪团伙的相互勾结[4]。一开始媒体渠道只是在构建叙事,还依然缺乏现在媒体报道常见的自信基调。在这样情形下的"网络战"的概念是非常有争议的,因为网络攻击并没有引起物理破坏和人员伤亡,犯罪者的身份也是未知的,这样的攻击只是引起短暂的功能失调而不是永恒的破坏。这些媒体数以倍计地夸大了信息,使得俄罗斯的网络战威胁成为了一个新的担心。随后由于故事的不断重复和进一步传播,有些新的片段和行为体不断出现,网络战慢慢就变成了一个既定事实。

来自俄罗斯和中国的黑客威胁似乎已经成为现在网络战相关报道中重复出现的主题[5]。许多美国媒体指责中国政府窃取美国情报的间谍行为,他们把这种网络窃秘和网络犯罪归类为网络战事件。2012年和2013年指责达到了顶峰。纽约时报发表了一篇来自网络安全公司麦迪安(Mandiant)的关于"APT1报告"的文章,文章对于中国政府的指责到了新的一个高度。除了网络战争,一些其他的表达也会在媒体报道中出现,例如"国家安全威胁"、"网络窃密"、"不对等网络战"、"激进的黑客活动"。这些词汇所隐含的负面属性和侵犯意义旨在让读者建立一种恐惧感和排斥感。上述第一种网络战叙事的基本目的是为了警醒读者小心"外来威胁"。

媒体报道的第二种叙事方式中,关注点不再是战争概念的本身而是对事件的深层次挖掘。Stuxnet蠕虫病毒(此病毒是一种网络武器,用于破坏伊朗的核项目)发现之后,这种叙事开始流行。自那之后,媒体报道了越来越多的类似的网络威胁题材,例如"Duqu"、"Flame"和"Gauss"病毒。这些叙事中一个特点是,因为"Stuxnet蠕虫"病毒是美国政府的产品,所以大多数媒体报道都宣扬这种病毒的复杂性以及它使得传统战争看上去很落后[6]。这种网络武器的危害叙事通过对于若隐若现的网络战争的灾难幻觉描述来吸引公众,让他们觉得这是一个数字黑暗时代的预兆。然而,尽管在报道中存在这种恐惧意识诱导,但是网络战叙事并没有引起太多反感,而是激起制造这种新型超级武器的欲望。因此,"Stuxnet蠕虫"病毒不仅仅是一个威胁,也是美国的网络空间霸权的代表。报道声称网络战争的影响力可能比"珍珠港"或者"9.11"事件的破坏力更大,引起的问题可能比核扩散还多[7]。在这样的叙事中,鼠标点击在任何一个技能娴熟的黑客手中基本变成了炸弹和子弹,然而事情远没有那么简单。

还有一种媒体报道的网络战叙事则试图减缓这样的大肆宣传,而是称网络战争还没有发生[8]。根据这种叙事,至今还没有具有破坏性结果的网络攻击,也没有足够的证据证明政府的参与,并且大多数发生的网络事件只是暂时的干扰而已。这些叙事表示,由于通过计算机网络操作没有造成人员伤亡和长期破坏,大多数所谓的网络战争其实只是网络犯罪或者是网络间谍活动。再者,这些叙事声称网络战争一词意义不大,因为网络攻击的威慑力没有那么强,破坏力也不大,因为其技术局限性使之无法引起严重的破坏[9]。除了美国以外,俄罗斯和中国也具备网络战能力,但是除非有冲突发生或者重要利益受到威胁,这些国家并不会轻易使用网络战武器。支持这种叙事者认为网络战争的

大肆宣扬是为了重构网络空间并且提供一种新的威胁以使人民更加顺从地接受监督[10]。尽管最后这种网络战叙事降低了网络威胁实际的危险性，但必须承认的是网络战争概念的不断出现已使之越来越流行，有些似乎已经有“既定事实”的支撑，尽管很少人会真正去讨论这些“既定事实”。

过去数年中，网络战常常成为新闻头条，似乎任何带有恶意的网络活动都被贴上了网络战的标签。这些例子如知识产权侵权、黑客组织活动、互联网审查和网络间谍等等，可见网络战叙事的界限非常模糊。尽管媒体倾向于建构故事旨在吸引读者，并获取他们的自身利益，但这并不是新闻记者的全部责任。事实上，专家和决策者这两个群体也制造了一些混淆，网络战争这一议题也需要专家和决策者们对之进行规范化。媒体基本是在回应他们的声音，同时提供一个更符合读者需要的受众材料。

1.2　决策者眼中的网络战争：国家安全问题　在美国的决策者眼中，网络战争对于国家安全是一种威胁。虽然不是所有决策者喜欢用“网络战争”这个具有争论的术语，但是网络威胁使美国的重要设施如电网和军事通信系统遭受威胁的观点正被广泛传播。普遍接受的观点是，通过网络攻击入侵美国公司和国防系统的国家，其目的是为了在网络战中获取优势，他们的行为正在侵蚀美国的权力。也有决策者声称，在最糟糕的情况下，网络战争或者网络恐怖攻击可能造成震惊全国的巨大损失。如同媒体报道一样，决策者构造的叙事在网络战争的概念中结合了网络犯罪和网络间谍行为。

理查德·D·克拉克(Richard D. Clarke)是《网络战争》(*Cyber War: the Next Threat to National Security and What to Do About it*)一书的作者，也是前白宫安全顾问。在其 2010 年出版的书中，他描述网络战争为“国家行为体或其代理人所发起或支持的未经授权侵入另一国家的计算机或者网络，或是影响计算机系统的任何其他行动，其目的是增加、改变、篡改数据、或引起计算机、网络系统或其所控制对象的功能瘫痪或者损坏”[11]。根据他的书籍，网络攻击被简单地认为和传统的武装攻击具有一样的破坏性的，最大的网络威胁来自于俄罗斯、中国和北朝鲜，而黑客是这些政府进行网络攻击的资源。2010 年，在五角大楼的国防网络受到外来威胁后，前美国国防部副部长威廉·J·林恩三世(William J. Lynn III)发表声明称美国将采取先发制人的网络空间战略，并命名网络空间为“第五战场”[12]。这个声明是在美国前国防部长罗伯特·盖茨(Robert Gates)刚下令构建美国网络司令部之后发表的。

理查德·克拉克还定义了“三位一体”的防御战略，用以保护美国主要的国家机器[13]。他建议美国政府控制一级互联网服务供应商并且建造一个深层数据包检查工具来监控通过国家网络的数据。他认为，尽管系统是自动化的，但仍需要人类干预来有效预警侵犯和不能低估的威胁。奥巴马总统也强调了国家安全局监控系统的必要性，他认为，“如果没有能力探测数字通信，我们就不能预防恐怖袭击或者网络威胁”[14]。事实上，美国国家安全局已经拥有这样的网络监控工具，正如棱镜门事件所揭露的那样，尽管许多人表达了对于民权侵犯的担忧。

虽然美国的决策者们在网络战争这个议题上的观点有轻微的不同，但网络攻击能够造成巨大破坏这个观念正在他们的叙事中不断重复。前国防部秘书长莱昂·帕内塔(Leon Panetta)声明说，一个巨大范围的网络攻击能够如“9.11”事件一样具有杀伤力。他相信，美国即将面临一个“网络珍珠港”，这个袭击“将会造成物理伤害和人员伤亡，会使国家机器瘫痪并震惊全国，从而引发强烈的美利坚脆弱感”[15]。帕内塔的声明变成了许多媒体报道的主调，为网络灾难的叙事提供了论据。

这些叙事表达的威胁包括网络恐怖组织或者像中国、俄罗斯和伊朗这些国家来源的网络攻击。尽管最初很少有决策者故意指控其他政府，但最近迹象显示了他们似乎基于所获取信息的越来越多的自信。国会议员迈克·罗杰斯(Mike Rogers)发表声明说，美国正失去对抗中国的网络战争优势[16]。奥巴马政府的国家安全顾问汤姆·多尼隆(Tom Donilon)称，来自中国的入侵是不能容忍的，中美双方政府应该就如何避免此事进行深入探讨[17]。这种叙事在 2013 年国会年度报告中达到顶峰，这一报告控诉中国采用计算机网络开发能力获取信息从而在危机时刻使中国人民解放军获益。虽然斯诺登揭秘使美国暂时沉默了一段时间，但最近美国司法部对五名中国军方人员的网络间谍活动指控再次使这一议题进入大众视线。美国决策者现在一个常见的观点是网络威胁需要政府介入才能实现国家利益的保护，并且网络安全优先程度需要提高。因此决策者一致倾向利用带有戏剧夸张和紧张局势色彩的叙事特征。这些声明有很多值得推敲的问题：一般的计算机网络入侵和工业间谍活动也往往被提升到网络战层面；报复成为了回应网络攻击的主要手段，而这会危害国家之间的关系；虽然近期的指控明确指向中国，但却没有足够的证据证明网络攻击有政府牵涉其中。事实上，网络安全问题牵涉到的主体很多，网络战叙事的构造还离不开 IT 技术人员和国际关系学者等专家，而专家们不同的背景和利益导向使网

络战叙事更趋混淆不清。

1.3 专家眼中的网络战争:多面议题 网络战争和网络安全具有多学科性质。来自不同背景的专家和学者对这个概念有不同的理解。比如说,"攻击"一词在国际法和网络安全中就不是同一个概念:对于一个国家而言,攻击意味着产生物理伤害或人员伤亡;而在一个网络安全专家眼中,任何恶意计算机入侵就是攻击。政策的制定正面临着一个挑战,即如何准确定义这些概念。专家们已经开始从跨学科角度和战略学、国际关系、国际法等不同角度探讨网络战争这个议题。

有人尝试通过创造一个跨学科方法来解决这个议题,但不尽如人意。其中一个尝试是《网络战入门》一书中从技术层面对网络战的解释和对国际关系面临的问题分析。此书作者们定义网络战争为"在网络空间中国家或者非国家行为者采取的政策延伸行动,要么是为了构建对另一个国家安全的严重威胁,要么是一国国家安全已经受到威胁的响应"[18]。这个定义的问题是安全本身被划分为几个不同层次,没有设定造成物理伤害或人员伤亡的限定条件,从而使这个定义过于宽广,几乎可以包含所有的黑客行为。在这些情况下,网络战争成为了一个网络空间内的混乱和危险的代名词[19]。

不同背景的专家对网络战争的战略意义有不同的分析。杰弗里·卡尔(Jeffrey Carr)是网络安全咨询公司(Taia Global Inc.)的创始人,他在美国陆军战争学院和美国空军技术学院发表演讲时声称,网络战争是真实的,在网络空间内发生的每一次操作都可能和某军事行动或者军事改革同步,可能促进军事目标的识别和攻击。尽管他所提供的支持证据是有争议的,但他的观点比较接近于战略学和国际关系研究领域的学者观点,他们大多认为网络战争是一种可支持物理攻击的方法。根据一位在兰德公司的资深管理科学家马丁·利比基(Martin Libicki)的观点,战争并不能只通过网络操作实施,要达到战争目的,国家仍然需要动用武装力量。网络攻击只能作为物理攻击的支持手段,而且网络攻击还需要足够的情报支撑。网络攻击的受害者也可能会故意隐瞒实情从而迷惑攻击者,而网络武器被发现后其有效性就会大大降低,因为网络武器所利用的漏洞可能会被修复,这种漏洞一旦修补后就会使之前使用的网络武器失效。网络威慑的可行性也不大,因为一个没有公开细节的威胁是非常难于让人相信的,而对细节的任何一个明示又可能使受害人马上加固自己的系统[20]。因此,对于利比基而言,网络战争是可能的,但对于国家来说想要过度依靠它会引起一定的风险,需要进一步评估网络战的复杂性。

在国际关系和战略研究领域,有一种关于中美网络战争的猜测。正如克里斯托弗·布隆克(Cristopher Bronk)在其文章"展望2020八九月份的中国网络战"("Blown to Bits: China's War in Cyberspace, August - September 2020")提到的,中国早已在战略性网络操作中是一个领先者,它的能力在于强大的防火墙可以将自己与其他国家隔离开来。作者于是推测中国和美国的网络战争的可能性,得出结论说,网络空间的攻击可能会造成意想不到的结果,并且国家会越发依赖这种手段以避免制裁和来自国际社会的指责。作者同时号召学术界、工业界和政府将必要的资源汇合起来共同防止这种意外结果的发生[21]。保护国家免受网络战争是"网络威斯特法利亚时代的来临"("Rise of a Cybered Westphalian Age")一文的中心主题[22]。在这篇文章中,两位作者支持在网络空间内构建边界,并建议网络司令部发展网络防御和攻击能力,开发网络威胁预警监控工具。

应对网络威胁不仅是能力问题,最需要的是能够有一个国际都能接受的统一标准来评价网络战争行为。然而,这些行为很难用现存的法律和规定来进行管理。事实上,国际法的专家已经尝试创建新的法律框架来解决这个问题。美国海军战争学院教授和国际法学者迈克尔·施密特(Michael N. Schmitt)为北约的一个项目制定了详细手册,即《塔林手册》(*Tallinn Manual on the International Law Applicable to Cyber Warfare*)。根据手册内容,能够引起系统损毁或者人员伤亡的网络攻击将被认为战争行为,一些产生同样后果的数据攻击行为也适用于此。许多专家同意说,如果系统损毁的修复需要物理硬件的替换才能实现亦应被认为是战争行为。因此,根据手册内容,造成系统受损且需要物理恢复的攻击将被认为是网络战争,但如果只是简单的软件重装就可以修复则不属于这一范畴[23]。这种网络战争的定义由于范围大为缩小更易避免混淆,应用性相对增强。

不同于决策者们相对统一的网络战叙事基调,专家们有不同的视角并对于网络战争有更深入的分析。尽管来自不同学科的专家们的观点有所区别,但是显而易见的是,相似的背景通常产生相似的叙事。一些学者和专家对网络战叙事的优弊各执己见,不同学科的讨论仍在不断继续。

2 网络战叙事的产生:表面和潜在动因

网络战争叙事的动因不仅是表达对于国家和社会安全的担心。创造这些叙事的主体拥有他们各自的利益,有的时候是共享的,有的时候是冲突的,有的已经明确表达,有的隐藏其后。大众媒体往往是在专家和决策者之后才讨论这个概念,但他们让这个概念流行

并且在公众意见中引起注意。在过去几年中，媒体报道的基调和频率明显有所变化，在决策者公开指责其他国家政府之前，媒体已经构建好威胁来自于外部的叙事。紧张局势成为报道的叙事基调，因为这类叙事迎合了喜欢戏剧性报道和暴力新闻的读者口味，从而可以为媒体带来更多的经济利益。当然也有一些报道指出这些言过其实行为背后的风险，但是他们的努力往往淹没在主基调的声音当中。

决策者的网络战叙事的表面动因往往是基于国家安全的保护，其中也包括经济安全，如对知识产权的合理保护。决策者致力于促进网络安全立法以保护这些安全利益。但利用网络战争来挑起实际上无关战争的议题，表明背后可能有其他的目的。例如，某一政策遭到了反对，因此需要一个叙事来帮助加速政策落实进程的发展。国家具有保护其人民免受外部和内部威胁的责任。不可否认的是，事实威胁的确会危害社会秩序与和平，为了证明一些行为或者政策的合理性，决策者需要强调威胁的害处，有时甚至需要夸大威胁使问题看上去足够严重或者危险。为了改变公众的认知，这些威胁需要让人足够信服。

“安全威胁的构建是一个需要安全化的过程，即让它成为‘对一个特定主体的存在性威胁’”，因此，“存在性威胁的构建意味着一种最高优先级和紧张气氛，如果这个问题没有得到解决，可能会引起致命的后果”。当帕内塔在对网络安全问题发表言论时，他所面对的是一群想要促进一些政策落实的商人，他希望通过制造紧张气氛以便让被民权组织例如 EFF 和 Avaaz 反对的《网络情报分享及保护法案》(CISPA) 这样的政策得以通过。他并没有隐瞒这一目的，他承认，“为了对我们的民主提供必要的保护，网络安全法律必须被国会通过。如果没有，我们是易受攻击的，国会必须有所行动，必须要有一个全面的法案”。为了制造一种紧张和紧急的感觉，为了加速政策制定的过程，他补充道，“我们没有其他选择，因为我们面对的威胁已经存在”[24]。但是，“将一些问题进行安全化的风险在于它给政府以特权并且为公民权利和自由的架空提供了合法性”[25]。网络空间的重建能够被私营企业利用来增加其实力，但也会给政府提供监管人民的工具。

专家们的网络战叙事也有许多不同的利益动机。一些研究是为了知识的增长或者为了给国家提供真实的、无偏颇的见解和建议。像利比基或施密特进行的研究就比较中立，他们认真深入地分析了网络战争问题。另一方面，不少网络安全专家卷入了一场巨大的利益冲突中。网络威胁应对政策一旦通过，网络安全专家们实际上可能是首先获利的，因为其他公司和政府需要他们提供服务。2014 年，奥巴马的财政预算中网络相关经费增加到 130 亿美元，同时联邦 IT 预算总共累积达到 820 亿美元[26]。在 APT1 报告发布后，麦迪安公司获得 10 亿美元的商业项目，使其总收入相对于上一年度增加了 60%[27]。其他公司也从资源重组中获取了大量利益，甚至给政府提供网络武器的黑市交易也在兴起[28]。更令人担心的是决策者现在正自己建立网络安全公司，其中一些正在为美国最大的国防承包商做说客。例如推动建立网络司令部的美国前美国国防部副部长威廉·J·林恩三世曾经是雷神 (Raytheon) 公司的说客。这个公司致力于提供军事通信、空军和导弹防御、雷达的电子系统以及网络安全和电子战解决方案。小布什政府的国土安全部长迈克尔·切尔托夫 (Michael Chertoff) 建立了自己网络安全咨询公司“Certoff Group”。霍华德·施密特 (Howard A. Schmidt) 是 2012 年 5 月之前的奥巴马管理团队中的网络安全协调官，他和 2005 年前第一任美国国土安全部长汤姆·里奇 (Tom Ridge) 一起建立了一个网络安全咨询公司，名为“Ridge Schmidt Cyber LLC”[29]。正因为这些，专家和决策者丧失了他们的公信力，因为他们为了自己的利益散播了令人混淆的叙事，动机是制造威胁以让别人更加依赖他们的服务和保护。这些决策者们的网络战叙事所暗示的方向某种程度上是他们个人利益的动机使然，因此越来越难分辨谁是真正的政策顾问，而谁是利益推销人员。

3　结　语

如上所述，基于不同的利益动机，媒体、决策者和专家这三个主体有着不同的网络战叙事。为了避免错误的网络战相关决策，三者需要加强沟通。专家们在避免国家间误解和一些问题的升级方面起着非常重要的指引角色。大多数关于网络战争的谜团只因为缺乏对于特定技术细节的理解才产生，正如乐尼·汉森 (Lene Hansen) 和海伦·尼森巴奥 (Helen Nissenbaum) 所指出的，“网络安全的技术性要求国际关系专家对于主流技术方法和问题有一定的熟悉度”[30]。一方面，国际关系专家和网络安全专家应充分交流与合作，以避免思维定势、思想偏见和意见混淆。另一方面决策者也需要对问题有更深入的理解，对传播关于外来威胁、灾难恐怖和双重标准的叙事进行风险评估。而将这些网络战叙事带到成千上万的受众面前的媒体，则应注意他们的叙事方式和风格，因为他们的选择很有可能会对世界造成未知结果的长期影响。

参 考 文 献

[1] Barbara Czarniawska. Narratives in Social Science Research [M]. London: SAGE, 2004: 17-20.

[2] John Arquilla, David Ronfeldt. Cyberwar is Coming! [J]. Comparative Strategy, 1993, 12(2): 141-165.

[3] Ibid, 31.

[4] John Markoff. Before the Gunfire, Cyberattacks [N/OL]. (2008-08-12) [2013-12-07]. The New York Times. under "Technology". http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[5] Conn Hallinan. Cyber War: Reality or Hype? [N/OL]. (2012-01-20) [2014-04-20]. The World Post. http://www.huffingtonpost.com/conn-hallinan/cyber-war-reality-or-hype_b_1219843.html.

[6] Ralph Langner. Stuxnet's Secret Twin: The Real Program to Sabotage Iran's Nuclear Facilities Was Far More Sophisticated Than Anyone Realized [J/OL]. (2013-11-21) [2013-12-10]. Foreign Policy. under "Exclusive". http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack#sthash.HQqRgcml.dpbs.

[7] Michael Joseph Gross. Silent War [J/OL]. (2013-07) [2014-04-20]. Vanity Fair. under "Hacking". http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business.

[8] Rid, Thomas. Think Again: Cyber-war [J/OL]. (2012-04) [2012-05-01]. Foreign Policy. under "Think Again." http://www.foreignpolicy.com/articles/2012/02/27/cyber-war.

[9] Henry Farrell. Cyber-Pearl Harbor is a Myth [N/OL]. (2013-11-11) [2014-04-16]. The Washington Post. November 11, 2013, under "The Monkey Cage." http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/11/11/cyber-pearl-harbor-is-a-myth/.

[10] Ryan Singel. Cyberwar Hype Intended to Destroy the Open Internet [J/OL]. (2010-03-01) [2014-04-15]. Wired. http://www.wired.com/2010/03/cyber-war-hype/.

[11] Richard A Clarke, Robert K Knake. Cyber War: The Next Threat to National Security and What to Do About It [M]. New York: HarperCollins, 2010: 70.

[12] William J. Lynn III. Defending a New Domain: the Pentagon's Cyberstrategy [J/OL]. (2010-10) [2013-12-08]. Foreign Affairs. under "Essays." http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

[13] Clarke and Knake: 160-178.

[14] Obama Speaks About Surveillance Changes [N/OL]. (2014-01-17) [2014-04-16]. CNN. under "Transcripts." http://transcripts.cnn.com/TRANSCRIPTS/1401/17/lvab.02.html.

[15] Council on Foreign Relations. Secretary Panetta's Speech About Cybersecurity [EB/OL]. [2012-10-15]. http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262.

[16] Mike Rogers. America is Losing the Cyberwar vs. China [EB/OL]. (2013-02-08). [2014-05-16]. http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=319502.

[17] Tom Donilon. The United States and the Asia-Pacific in 2013 [EB/OL]. (2013-03-11) [2014-05-16]. The White House. http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

[18] Paulo Shakarian, Jana Shakarian and andrew Ruef. Introduction to Cyber-Warfare: a Multidisciplinary Approach [M]. Waltham MA: Elsevier 2013: 2.

[19] Serge Malenkovich. Look at Cyberwar With Your Own Eyes: An Interactive Map of Online Threats [EB/OL]. [2014-05-16]. http://blog.kaspersky.com/look-at-cyberwar-with-your-own-eyes-an-interactive-map-of-online-threats/.

[20] Martin C. Libicki. Cyberdeterrence and Cyberwar [EB/OL]. [2012-10-30]. RAND, 2009. http://www.rand.org/pubs/monographs/MG877.html.

[21] Christopher Bronk. Blown to Bits: China's War in Cyberspace, August-September 2020 [J]. Strategic Studies Quarterly, Spring 2011: 1-20.

[22] Chris C. Demchak and Peter Dombrowski. Rise of a Cybered Westphalian Age [J]. Strategic Studies Quarterly, Spring 2011: 32-61.

[23] Michael N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare [M]. New York: Cambridge University Press, 2013: 106-110.

[24] Council on Foreign Relations. Secretary Panetta's Speech About Cybersecurity [EB/OL]. [2012-10-15]. http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262.

[25] Barry Buzan and Lene Hansen. The Evolution of International Security Studies [M]. New York: Cambridge University Press, 2009: 217.

[26] Mohana Ravindranath. Obama's Budget Proposal Would Increase Spending on Cybersecurity [J/OL]. (2013-04-15) [2013-12-21]. The Washington Post. under "On IT." http://www.washingtonpost.com/business/on-it/obamas-budget-proposal-would-increase-spending-on-cybersecurity/2013/04/14/218e71d6-a2b8-11e2-be47-b44febada3a8_story.html.

[27] Associated Press in Washington. China Hacking Claims: Tech Firms Move to Front Lines in U.S. Cyberwar [N/OL]. (2013-02-21) [2013-12-20]. The Guardian. under "China." http://www.theguardian.com/world/2013/feb/21/china-hacking-claims-tech-firms.

[28] Lillian Ablon, Martin C. Libicki, Andrea A Golay. Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar [EB/OL] [2014-04-30]. RAND. 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

[29] http://www.ridgeschmidtcyber.com/ (accessed December 21, 2013).

[30] Lene Hansen, Helen Nissenbaum. Digital Disaster, Cyber Security and the Copenhagen School [J]. International Studies Quarterly, 2009(53): 1172.

(责编: 贺小利)