序形成扰乱因素。[①] 网络俨然成为军事领域攻防的新型战略工具与非军事领域竞争的新型筹码，是达到军事威慑、战略瘫痪、政治警告、经济封锁、文化同化、政局动乱、舆论操控、社会分裂等综合目标的强有力工具。因此，网络安全关涉的领域既涵盖国家军事安全方面，也涉及非军事安全领域；既利用非传统安全的手段实现传统安全之目的，又利用传统安全手段实现非传统安全之目的；其演变过程既存在非传统安全向传统安全的转变，也存在传统安全向非传统安全的转变；其参与主体既有国家行为体，也有非国家行为体；目标设定上既有对国家政权的指向，也有对个人或组织的指向。总之，其凸显了非传统安全与传统安全相互交织的特征。

从非传统安全研究的角度看，网络安全是信息时代非传统安全的重大议题之一，既挑战了非传统安全研究的固有思路，也为非传统安全研究呈现了新的时代元素。现有非传统安全研究一般对非传统与传统安全进行手段、主体、维护方式等的明确二元界分，[②] 更多地将非传统安全置于与传统安全相互独立或对立的关系。这在非传统安全产生伊始和非传统安全研究发轫之际，有利于非传统安全理论体系的形成和提升公众对非传统安全问题的关注，且在分析常规性非传统安全问题时具有指导力与解释力，然而在分析网络安全、生物安全、能源安全、恐怖主义等明显带有传统安全元素的非传统安全问题时，这种对非传统安全－传统安全作非此即彼、彼此独立或对立的思路已受到挑战，而从传统安全与非传统安全紧密交织、相互转化的关系进行细微分析应是理论研究的必然转向。本文突破对非传统安全进行层面（个人－社会－国家－区域－全球）、领域（军事－经济－政治－社会）、价值（人的安全－社会安全－国家安全）研究的惯常作法，而专从非传统安全与传统安全多重交织的角度，提出“‘多元性’非传统安全威胁”的概念。

二“多元性”非传统安全威胁：内涵、特征与挑战

（一）“多元性”非传统安全威胁的内涵与特征

从词义上看，“元”一般用以表达一种根源性、原本性或始发性，或者说，其根本含义具有一种不可替代的“本体性”。“多元性”非传统安全威胁是指与传统安全要素多重交织的威胁。其中，传统安全要素在主体、手段、意图等方面具有军事性与政治性，如在当前引起普遍高度关注的生物安全威胁中，生物技术的开发与应用已大量服务于军事与国家安全战略，一些别有用心的国家与组织凭借其先进的生物技术，以生物物种入侵、重大传染病、生物暴力等为“生物武器”，“静悄悄”地

① 王军:《多维视野下的网络战：缘起、演进与应对》，载《世界经济与政治》，2012年第7期，第80-98页。

② 余潇枫、潘一禾、王江丽：《非传统安全概论》，杭州：浙江人民出版社2006年版，第55页。

推进其军事或政治计划。[①] 关于非传统与传统安全相互交织、相互转化，中国高层已有明确判定，如中国共产党第十六、十七、十八大报告就指出中国正面临传统安全威胁与非传统安全威胁“相互交织”的挑战；研究者也有相关分析，如姜维清提出“交织安全”并认为是威胁国家的“第三种威胁”[②]，余潇枫概括了其多种表现形式，[③] 还有学者基于相互交织的现实而提出军队要加强“多样化军事行动能力”[④]。

“多元性”非传统安全威胁除具有突然爆发性、广泛破坏性、普遍威胁性等非传统安全威胁的一般特征外，更为特殊的是，其与自然灾害、重大事故性灾难等常规非传统安全威胁相比，突出表现为非传统与传统安全威胁的多元因素相互诱发、相互交叉、相互交混、相互交叠与相互转化，这些因素包括诱因、意图、主体、手段、领域、目标、地缘、过程、属性等；在表现形式上，或以传统安全手段达到非传统安全目的（如反恐战争、网军、非战争军事行动），或以非传统安全手段解决传统安全问题（如生物战、网络战）。

从全球范围看，典型的“多元性”非传统安全议题包括核安全、能源安全、网络安全、反恐安全、生物安全等。其与传统安全、非传统安全的关系参见图 1。[⑤]

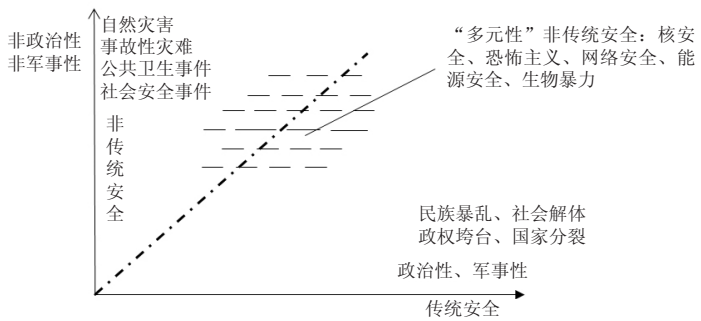


图1 传统安全、非传统安全、“多元性”非传统安全的大致分类图

① 贺福初、高福锁：《生物安全：国防战略制高点》，载《求是》2014年第1期；于晓峰：《生物恐怖：21世纪国家安全的新威胁》，载《中国国防报》，2002年6月4日，第4版；彭海、张凤坡：《生物国防防范悄无声息的战争》，凤凰网，http://finance.ifeng.com/a/20131029/10953740_0.shtml。

② 姜维清：《交织：国家安全的第三种威胁》，北京：世界知识出版社2011年版。

② 余潇枫：《中国非传统安全研究报告》，北京：社会科学文献出版社2012年版， 总论。

④ 李承：《应对传统安全与非传统安全威胁的统一——新时期军队历史使命的延伸》，载《军事历史研究》，2007年第4期，第17-22页； 钟远腾：《提高多样化军事行动能力》，载《中国国防报》，2010年6月7日，第3版。

⑤ 作者认为，需要特别指出的是，核安全、能源安全、网络安全等在很多方面呈现了传统安全的特征，但在归类上（如果一定要归类的话）又不适合划入严格意义上的“传统安全”的范围。本文基于以下考虑将之归为非传统安全：一是全球各领域各层面对和平、发展与安全的普遍期许，二是与冷战之前相当长的历史时段内的大规模武力战争之境况相比，环境、灾害、贫困等“非武力对抗性战争”威胁已开始变得广泛与紧迫，三是在威胁应对方式上，政策领域对“非战争军事手段”的采用愈加制度化、程序化；在理论研究领域，将具有传统安全元素的威胁划入“非传统安全”的边界内，客观上对政策界施以“去军事化”、“去政治化”的解决途径给予了取向上的向导，更加符合当前国际社会对军控与战备的整体要求（图1为作者自制）。

以网络安全威胁为例，“多元性”非传统安全威胁的特征表现为：

第一，主体多样性与领域多向性，即国家与非国家、组织与个人、官方与非官方、主动与被动等多样化主体，而这些主体的多样既指威胁的施动身份，也指威胁的受动身份；威胁领域覆盖了高政治与低政治、军事与非军事等多方面。以黑客（hacker）为例，其原本只是一种技术身份，当其被运用于军事、政治领域时，就成为国家安全的重大潜隐性威胁。黑客的组织与发动主体可以是个人，也可以是组织（国家的或非国家的），其威胁对象则包括了一切接入网络终端的用户。一般而言，黑客行动一般指有组织或无组织地利用恶意代码、置入程序、网络武器[①] 等对目标进行肆意破坏的行为，既存在于国家间“网络战”中对关键军事系统的破坏，也存在于民事性网络犯罪中的信息盗窃、网络欺诈与恶意篡改，还存在于社会网络战争中带有民族主义情绪的对目标信息网络的警告性破坏。黑客攻击是当前各国的普遍性共同威胁，据权威机构测算，自 21 世纪始，平均每个宽频用户每天会遭受 10 个以上的黑客攻击；[②] 中国国家互联网应急中心统计显示，2012 年“幽灵躯壳”、“匿名者”、“反恐黑客”、阿尔及利亚 Barbaros-DZ 等黑客组织频繁发动对中国的网络攻击，“匿名者”还宣称要对中国多家政府和大型企业发动攻击，大数据和云平台运用中遭受的恶意代码、信息窃取、网络欺诈等构成了中国网络空间安全的巨大挑战。[③] 尤为特殊的是，在网络安全威胁的制造者中，有些主体是在不自觉、甚至是不知情的情况下成为这条“主体链”中的一员，如有研究就分析指出，在网络攻击者匿名、网络空间互联互通、归因溯源技术受限的情景下，本来身处局外的“第三方”通常被诱导或欺骗或在完全不知情的条件下“被成为”网络空间威慑中的“局外合作者”[④]。

第二，动因多源性与目标多重性，即网络安全威胁的发起动因极为综合复杂，既因军事报复、政治对抗、宗教差异等引起，也因历史记忆、认同差异、贸易壁垒等引发；在目标上，通过各类网络威胁以达到军事威慑、战略瘫痪、政治警告、经济封锁、文化同化、社会恐慌等综合性目标。网络恐怖主义是网络安全威胁中极为特殊的一类，虽然研究者和各国官方文件对其形式、主体、手段等有不同认定与立场，

---

① 美国国家审计署的《信息安全：对于国防部的计算机进攻构成越来越大的威胁》称，全世界有120多个政府在开发进攻性战略信息战武器；仅在1995年，美国国防部可能遭受25万次袭击，而每150次袭击中只有一次被侦测到且被报告。参见张召忠：《网络战争》，北京：解放军文艺出版社2001年版，第36页。

② 卢新德：《构建信息安全保障新体系——全球信息战的新形势与我国的信息安全战略》，北京：中国经济出版社2007年版，第78页。

③《2012年我国互联网网络安全态势综述》，国家互联网应急中心，http://www.cert.org.cn/publish/main/upload/File/201303212012CNCERTreport.pdf。

④ 董青岭：《网络空间威慑，如何推进第三方责任》，载《世界经济与政治》，2013年第9期，第113-124页。

但一般认为它是通过网络空间实施对国家、社会或公民的危害行动及相关活动（如动员、宣传与交易等）。被美国评定为活跃的恐怖分子组织的 40 个机构已拥有 4 300 个以上的网站，[①] 多数网站介绍了制造炸弹、引爆汽车及杀害人质的方法；[②] 美国国会公布的 30 个恐怖组织中，12 个建有互联网主页。网络恐怖主义在未来将呈现行动更隐蔽、防范更困难、攻击更有效、后果更可怕的趋势。[③] 恐怖主义常与战争、暴乱及革命等“暴力”联结在一起，被视为一个“暴力行为体系”，[④] 而网络恐怖主义则利用网络平台实施恐怖行动，两者在根本动因与目标上具有一致性，即大都出于国际政治秩序不平等、西方大国对伊斯兰国家的践踏、历史记忆与民族情绪、文明与宗教差异、贫富差距等综合原因，而意欲通过网络恐怖行动而达到报复、施压、威慑、警告、颠覆等综合目标。

第三，地缘多源性与空间多维性，即“多元性”非传统安全威胁源于国内、国际、边境等多样的地缘因素，且在信息化、全球化的助推下瞬间成为跨国、跨区域性的威胁。网络威胁由于其技术门槛低（只要能接入互联网），导致其在任何一个空间点上都能实现对位于其他空间点的目标的攻击，完全突破传统作战当中的空间与地缘上的限制，且易攻难守。在国家间军事性的“网络战”中，“网络”或“信息”成为一种作战武器，而形成一种以使对方网络防御与监测系统瘫痪为目标的作战形态，并成为蔓延全球的“新型战争”（new wars）。“网络战”与电子战、心理战、情报战共同构成了现代“信息战”[⑤] 的主要形式。在 1991 年海湾战争中，美军通过病毒芯片调换伊拉克的打印机芯片，导致伊拉克整个防空系统的预警与 C^4I 系统瘫痪，网络战的雏形出现；1999 年科索沃战争中，美军成立了“网上作战小组”，正式宣布使用了“网络战”，美国与南联盟、俄罗斯相互对对方的指挥控制网、通信与情报系统、大型公用商业网等反复进行宣传攻势与黑客攻击，导致双方的关键信息网络严重瘫痪；在 2003 年伊拉克战争、阿富汗战争中，美国成立网络联合特种作战部队，专门负责网络攻击与防护。[⑥] 网络战的实施者通过网络而建立跨空间、跨地域性组织，使得本国与他国的地域性与空间性障碍完全消失；通过信息技术与网络平台使

① 史先涛：《因特网成恐怖分子重要工具》，载《参考消息》，2006年5月12日，第3版。

② [墨西哥]埃里克·莱赛：《“网络反恐”已成当务之急》，载《参考消息》，2005年8月9日，第1版。

③ 卢新德：《构建信息安全保障新体系——全球信息战的新形势与我国的信息安全战略》，北京：中国经济出版社2007年版，第91-94页。

④ [美]欧文·沃尔：《恐怖主义与国际关系》，载[美]威廉·奥尔森：《国际关系的理论与实践》，王沿等译，北京：中国社会科学出版社1987年版，第520页。

⑤“信息战”最早由汤姆·罗那在1976年提出，指决策系统之间的斗争；美国未来学家托夫勒将之界定为“对战争、冲突和作战的一种想法”，是一种“新的战争形态”。参见王保存、刘玉建：《外军信息战研究概览》，北京：军事科学出版社1999年版，第84页。

⑥ 陈岸然、王忠：《信息战视野中的典型战例研究》，上海：学林出版社2009年版，第56-69页。

得“网络武器”有能力远距离攻击目标，实现空间上的轻易跨越而成为跨国性、区域性的威胁，而这是传统机械化战争所无法达到的。

第四，手段多样性与过程多变性，即网络安全威胁的实施手段包括军事、政治、经济、文化、信息、舆论、技术等综合化的方式，其产生、发展与演化的整个过程呈现单一与复合、简单与复杂、常态与非常态危机的交替转化与相互诱发。2013 年“斯诺登事件”中，一项发起于个人的信息披露行动，瞬间升级为一场国家间信息安全保障能力的较量、一场关于网络空间是否安全的辩论、一场世界组织关于人权的抗争、一场国家安全防御与冲突升级的博弈、一场外交规范与姿态迅速调适的演练。又如 2001 年中美南海撞机后，中美各自网络黑客来回互攻而形成“第一次世界黑客大战”[①]，美国黑客扬言要向中国发起“网络战争”，大量官方与民间黑客入侵中国官方网络系统，导致中国 40 多家网站关闭，200 多个网页被涂改，而中国黑客则以“网络卫国战”回击，致使白宫网站关闭 2 小时，中美黑客的相互攻击导致威胁升级，使得这场发起于民间黑客攻击的威胁演变成国家之间的政治对抗。在这场典型的“社会网络战”（netwar）中，民间或政府行为体为维护国家主权、特定利益、民族认同而发动具有民族主义、意识形态特征的集体性吁请与抗议，后演化为国家层面之间的政治对抗与博弈。

（二）“多元性”非传统安全治理的困境

第一，边界模糊与动态，难以界定“主权”。与陆、海、空、天等领域相比，网络虚拟空间边界模糊与开放、甚至无所谓边界，且时刻处于高度动态与变化当中。信息战“没有国界和前后方之分”[②]；“网络无国界”，由铁丝网、高筑墙、界碑等构筑的国界在网络安全威胁下开始变得愈加模糊与不重要。[③] 这导致无法对网络空间内的权利与利益进行“主权”声明，也无法对其进行“领土”、“领空”、“领海”等的划定，这导致网络安全治理中存在诸多不确定性、模糊性与争议性。

第二，法律与规范缺失，难以判定“合法性”。网络安全威胁在呈现形式与具体实施上突破了传统意义上的实体性威胁，因而在内容、解释、具体规定等方面对相关国际法提出了挑战。现有国际法律法规（如《国际武装冲突法》）虽在某些方面为网络安全威胁的预防与反应给出了原则性依据，但在更多具体细节上尚“无法可依”，如无法根据确切、共同认可的标准对国家间军事武力对抗中的网络“威胁”进行“身份”认定（恐怖分子或非恐怖分子，军人或平民）或“合法性”标准的判定（威

① 美国记者Craig S. Smith称此黑客互攻为“第一次世界黑客大战”，参见Craig S. Smith, “The First World Hacker War,” *The New York Time*, May 13, 2001。

② 卢新德：《构建信息安全保障新体系——全球信息战的新形势与我国的信息安全战略》，北京：中国经济出版社2007年版，第11页。

③ 张召忠：《网络战争》，北京：解放军文艺出版社2001年版，第21-25页。

胁本身是否合法、应对手段是否合法），也无法对“和平”条件下的网络攻防、网络犯罪、社会网络战、网络恐怖主义等行动进行治理与应对手段上的规范。国际法相关内容的缺失或不确切导致的一个根本难题是：在网络安全威胁应对及其本身是否是“威胁”的判定上，都带来极大争议。如2013年斯诺登事件后，美国以“双重标准”就此网络行动进行辩解。①

第三，空间具有跨越性，难以跟踪“过程”。一是空间与国界的跨越性。“网络战”以虚拟化的“网络”为新型载体，具有“非接触性”特征，从“平台中心战”转向了“网络中心战”，即不跨越他国地理边界便可对他国进行信息瘫痪及由此而导致的战略瘫痪，彻底实现了“运筹帷幄而决胜千里”的力量格局与作战手法转换，导致难以追溯其“过程”。二是多个国家自觉或不自觉地成为网络安全威胁链条中的一环，“第三方责任”模糊且难以认定。研究者假定了这样的“第三方责任”情景：“A国恐怖分子、情报机构、激进团体或黑客个人劫持了第三方C国的计算机系统并途经D国的信息通讯网络对B国发起持续且破坏性巨大的网络进攻，而B国通过自身或盟国先进的网络溯源技术追踪探测到了攻击源来自C国和D国”，② 那么B国跨越自身国界对C国或D国进行反击的“合法”路径是什么？ C国或D国作为“第三方”的“局外合作者”是否承担责任，又以怎样的方式承担怎样的责任？网络安全威胁在虚拟平台上的空间跨越及其过程中不同主体的复杂关系，大大增加了溯源难度。

第四，行为体多样与多变，难以确定“身份”。如前所述，网络安全威胁的施动者与受动者都具有多样性的特征，在主动或被动两类上，施动主体包括国家与非国家、组织与非组织、集体与个人等，而受动主体则包括了一切接入网络终端的用户，包括个人、组织与国家，而又由于军事、政治、外交等信息的涉密特征，导致一些网络安全威胁具有神秘色彩，无法确定施动者或受动者的身份。主客体的“不明身份”导致网络安全威胁与应对在信息、力量、格局上的“不对称”，常规性应对举措常常无法有效应对。

第五，发生发展过程潜隐性大、突发性强、复杂性高，难以通过单一国家、单一部门、单一手段进行应对。很多网络安全威胁，如黑客、社会网络战和网络恐怖主义行动，都带有强烈的意识形态和民族主义倾向，目标是为摧毁“敌对目标”的权力堡垒，或形成压力以迫使敌对方做出政治、军事或外交上的新改变；一些个人或社会组织还利用网络针对战争、核武、宗教、人权、环境、妇女等问题对相关国

---

①《斯诺登事件暴露美双重标准》，中国法院网，http://www.fzwgov.com/Article/Html/2013/07/15_507763.html。

② 董青岭：《网络空间威慑，如何推进第三方责任》，载《世界经济与政治》，2013年第9期，第113-124页。

家或团体进行舆论施压，形成强大的舆论与心理导向。同时，这些网络安全问题一般都具有潜隐时间长、影响面广、爆发突然、控制难度高等特征，因此这类威胁的治理对战略布控、领导指挥、信息搜集、人力部署、技术支持、国际合作等方面提出了特别高的能力要求，需要信息、法律、公安等多部门的有效联动与迅速响应，必要时还需要国防与军队部门的参与，这无疑增加了治理难度。

三“优态共存”:“多元性”非传统安全治理的较优路径

在网络安全维护中，当前多数国家采取了“进攻型”战略，如2010年美国发起以“控制－塑造”为基本特征的“进攻型互联网自由”战略（Offensive Internet Freedom Strategy），[①] 建立网络司令部（cyber command）作为网络战的指挥机构，专攻网络防御和网络渗透作战，推进信息化条件下的实体战场转向网络空间战场；[②] 日本奉行“进攻－防御”型战略以抢占网络高地；[③] 欧盟与俄罗斯则分别建立“集聚型”和“综合型”信息安全战略模式；[④] 美、日、俄、英、韩、印等国家还分别组建进攻型的网络安全推进机构与网络作战部队。[⑤] 各国的网络安全举措在无形中加速了网络战的冲突升级与安全困境，如有研究者指出，美国奉行的进攻型网络战带有致命性缺陷，甚至会“引火烧身”[⑥]。

“优态共存”建基于安全与伦理之关系，以“类伦理”为衡量尺度与精神体现。类伦理是一种以人类共同体为整体价值尺度的道德理性，是依照人的类本性、类生活、类价值的要求所确立的人类活动的终极准则；类伦理在人、社会、国家、国际、全球的类关系上蕴涵着人的全部交互关系的整体性统一、历史的否定性超越与跨越国界、超越种族的丰富性和谐。[⑦]

---

① 沈逸：《应对进攻型互联网自由战略的挑战——析中美在全球信息空间的竞争与合作》，载《世界经济与政治》，2012年第2期，第69-79页；美国一些研究者也提出，由于美国的非对称性脆弱（asymmetrical vulnerability），美国应在网络空间的争夺中采取更加进攻型性的对策。参见Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do about It*, London : Harper Collins, 2010。

② 吴清丽、王君学：《世界网络战部队的发展现状》，载《红旗文摘》，2010年第21期，第34-36页。

③ 高望来：《日本抢占网络高地》，载《世界知识》，2012年第4期，第28-29页。

④ 卢新德：《构建信息安全保障新体系——全球信息战的新形势与我国的信息安全战略》，北京：中国经济出版社2007年版，第169-199页。

⑤ 魏岳江、薛玉忠、孙立华：《世界各国的网络作战部队》，载《国防科技工业》，2011年第7期，第85页。

⑥ 倪海宁：《美军“网络战”理论与实践》，载《国际资料信息》，2008年第7期，第14-18页。

⑦ 余潇枫：《从危态对抗到优态共存——广义安全观与非传统安全战略的价值定位》，载《世界经济与政治》，2004年第2期，第8-13页。

优态共存主张“共同认同”和“互惠共建”，以社会共有、权利共享、和平共处、价值共创为理性法则。若从生存状态的“优化”角度来关注安全及其价值目标，人的生存状态可以分为四个层次：优化状态、弱化状态、劣化状态和恶化（危险状态），这四种状态与威胁的联结可推演出四种威胁状态：没有威胁、有潜在威胁、有间接威胁和有直接威胁。倘若视“直接威胁”是典型的“危险状态”，那么“生存优态”就是“没有威胁”，即“生存优态”才是真正的安全状态。因此，安全可被视为是行为体间的“优态共存”。[①] 传统战略研究将安全维护设定为“威胁－对抗”、“你不安全我才安全”的“危态对抗”的逻辑，而“优态共存”以“认同共享”和“互惠共建”为实现方式，代表一种全新的安全哲学理念。

其一，“优态”是安全建构的理想状态，表征是安全行为体可持续发展的状态。“优态”牵引了国际关系主题的转变，即从“战争与和平”转变到“和平与发展”，又再次发展到“安全与发展”。从安全的观察角度出发，和平与发展并非直接带来安全，相反在很多情境下，和平掩盖了不安全，发展制造了不安全。如巴里•布赞（Barry Buzan）在论述结构暴力（structural violence）时指出，即使在没有战争的状态下，全球及国内经济结构、分配机制等现存的各种制度结构已经构成了人的生存与发展的威胁，因而成为各种安全问题的引发因素。同时，伴随着人类社会的发展而引发的各种安全问题也层出不穷，如环境恶化问题、资源短缺问题、文化认同问题等。因此，“优态”为安全的建构提供一种可以容纳和平、发展与安全之时代主题词的新理念。

其二，“共存”（coexistence）是“优态”获得的条件与方式，摒弃了“危态对抗”情境下对敌人的假想与恶意的主观设计，取而代之的是“自者”与“他者”的“和合共建”。概括起来，人类的安全维护模式主要有五种：[②] 一是“隔离防守式”的安全模式，通过寻找天然的或建立人为的“篱笆墙”来阻挡敌人的进攻，是国家面临危险时最传统、也最为惯用的安全防护策略。这种安全模式信奉“我的安全重于你的安全”观念；二是“进攻拓展式”的安全模式，通过主动出击、先发制人来取得自身安全，反映的是“危态对抗、强者为王”的安全理念，属于“你不安全我才安全”的心态；三是“结盟协作式”的安全模式，重视国家安全的相对获益，选择相互立信守约、互为盟友的方式来避免现实的或想象的冲突。这种安全模式反映的是“安危与共、进退同步”的安全哲学理念，表现的是“你不安全我也不安全”的心态；四是“集体防御型”的安全模式，通过建立集体防御性机制来共同维护集体的安全，以最终保护自身安全，反映的是“大家安全我

① 余潇枫、潘一禾、王江丽：《非传统安全概论》，杭州：浙江人民出版社2006年版，第353页。
② 余潇枫、潘一禾、王江丽：《非传统安全概论》，第361-362页。

才安全”的心态；五是“和合共建式”的安全模式，通过在主体间营造彼此信任、共同维护的“共同认同”，以达到“不谈安全而达到安全”的状态，反映的是“优态共存、顾全本土”的安全理念，表现的是“你安全我才安全，我安全你也才安全”的心态。综合比较而言，“和合共建式”的安全维护模式建构安全的稳定性、长久性、可持续性都要优于其他模式。

网络安全中的主权难以界定、合法性难以判定、身份难以限定、过程难以确定、单一行为体无法有效治理等挑战，决定了网络安全挑战与能力之间具有鲜明的“非对称性”，挑战了现有的非传统安全治理理念与方式。从本质与长远看，“优态共存”在三个方面更好地适应了网络安全治理的核心能力要求。

第一，跨界合作，即各主权国家、国际组织实现互利共赢、协商对话的平等合作。这可从三方面来看，一是全球网络空间具有共有共创共享与互通互联互感的特征，因而是一个利益整体，也因而决定了任何先发制人式地攻击全球信息空间都会导致自身利益受损，也还有极大可能遭致反击从而导致所有关涉主体都陷入安全困境；二是从战争形态看，网络战与以往战争的最大区别，就是战争武器可在更大范围内通过虚拟空间自由联结、互动；传统意义上区分明显的战略、战区、战场、战士等不同层面的联系更加紧密；战争进行方式也由兵力与兵力的对抗转变为体系与体系的对抗；[①] 三是网络空间具有极端脆弱性，易攻难守，重建网络比组建网络来得更难，进攻性网络攻击行动带来的反击预期，让进攻性行动变得更加谨慎。上述原因决定了一些国家奉行主动进攻型网络安全战略必定破坏全球虚拟空间的自由、公平与文明，不构成网络安全维护的最优“策略”。从长远与全球看，合作是针对网络虚拟空间的最优策略。网络安全中的跨界合作，既包括跨“硬边界”（hard boundary）的合作，即跨越陆、海、空、天的边界，还包括跨“软边界”（soft boundary）的合作，即跨越信息边界、利益边界、文化边界、认同边界的合作。这需要世界各国、各组织不能仅从自身利益来考虑网络安全，而需站在全球空间自由与安全的角度，必要地限制与规范自身网络行为，共同维护全球网络安全。

第二，建立“大安全”理念，即有必要突破传统与非传统安全的固有界分，从传统安全及其与非传统安全相互交织的角度来看待“多元性”非传统安全，建立涵盖国际安全、国家安全、人的安全的“大安全”理念。其实施包括两方面：一是在研究上，要基于非传统安全与传统安全相互交织的角度重新看待非传统安全研究。既要注重传统安全与非传统安全的区别与各自特征，查找非传统安全异于、对立或独立于传统安全的相对独立性，通过划分两者的明确边界来提升非传统安全的相对

① 吴清丽、王君学：《世界网络战部队的发展现状》，载《红旗文摘》，2010年第21期，第34-36页。

新颖性、独特性、优先性，又不应忽视二者相互交织的特性及其带来的复杂性、综合性、全局性，要将非传统安全研究与治理实践置于“进攻-防御”、“军事”、“武力”、“对抗”等仍普遍存在与奉行的传统安全之现实中，提高多元性非传统安全维护的针对性、切实性与有效性。非传统与传统安全理论分析的相对独立倾向与现实中非传统安全与传统安全相互交织、相互联结的现实，值得当前非传统安全研究者深刻把握。二是在安全治理实践上，要重视国家安全、社会安全与人的安全三者之间的优先次序与路径差异，要十分重视人的安全与需要。不同类型的网络安全威胁影响到不同层面的安全，直指国家军事核心的威胁需以国家安全为中心，限于社会领域的网络安全威胁要以维护社会秩序与维持社会结构为重心，而不论是哪个层面的威胁，都应充分考虑人的安全与发展需要，以人的安全（human security，或译“人类安全”）为终极目标。“多元性”非传统安全关涉到国家与社会的不同层面与领域，需要整体性、全局性与协同性的安全观，在价值定位上要以人的生存、生活与发展为中心，在国家安全与社会安全维护中要分清两者的优先次序与各自的路径差异。

第三，超越安全困境，即要超越“你不安全我才安全”、“我的安全导致你不安全”的“安全困境”。“在世界政治的所有困境中，安全困境是非常重要的。它直指国际政治理论与实践的核心”。[①] 安全困境的核心观点认为，一国维护自身安全的行为会招致他国猜疑，而引发他国加紧进攻或防御的举措，这一反复过程将导致所有关涉国家陷入愈加对抗与冲突的“困境”之中，如损害他国安全、集体受损、意图的不可确定、无法做出最满意决策。[②] 在网络安全领域，自我感觉网络不安全的国家更易倾向于进攻型策略，这导致他国采取防御－进攻型的应对策略，因而酿成网络世界的“安全困境”。关于如何超越安全困境，国际关系、国际安全等相关领域的研究者有不同设想，如巴里·布赞提出“成熟的无政府”（mature anarchy）[③]；罗伯特·杰维斯（Robert Jervis）建构“安全机制”（security regime）[④]；卡尔·多伊奇（Karl Deutsch）提出“安全共同体”（security community）[⑤]；以温特为代表的建构主义学者则提出通过语言、认知与互动的反复进程而建构安全观念；[⑥] 董青岭基于工具理

① 尹树强：《“安全困境”概念辨析》，载《现代国际关系》，2003年第1期，第57-61页。

② Alan Collins, *The Security Dilemma and the End of the Cold War*, Keele: Keele University Press, 1997, pp. 11-14.

③ Barry Buzan, *People, State and Fear, An Agenda in International Security Studies in the Post-cold War Era*, Hemel Hempstead: Harvester,1991, p. 177.

④ Robert Jervis, “Security Regimes,” *International Organization*, Vol.36, No.2 (Spring 1982), pp. 357-378.

⑤ Karl W. Deutsch, Sidney A. Burrell, Robert A. Kann, et al., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton: Princeton University Press, 1957, p. 5.

⑥ Alexander Wendt, “Anarchy is What States Make of It: The Social Construction of Power Politics,” *International Organization*, Vol.46, No.2 (Spring 1992), pp. 391-425.

性假定和风险偏好分析提出了“理性网络空间威慑模型”[①]。这些不同主张在解释与摆脱安全困境的实践上都有各自特定的价值，然而网络安全议题具有边界开放、接入自由、易攻难守、跨越时空等特性，突破了已有国际关系研究对权力、等级、攻防的理论假定，网络安全治理不能遵循你死我活、进攻－防御－威胁升级－安全困境、“你不安全我才安全”的零和或负和博弈的固有思维，而需要一种以合作、互利、共赢为目标的新思维。“优态共存”倡导“你安全我才安全”与“和合共建”的安全哲学新理念，除考虑同质性冲突的解决，尤其重在对异质性冲突的理解与应对，倡导“共建共赢”与“优态共存”基础上的“共享安全”。[②]“多元性”非传统安全战略的价值定位也只有确立在“共优”范式上，才有其全球可持续发展的意义。

综上所述，网络是一把双刃剑，在增进主体间相互交流与了解、创造国际关系新的空间与手法的同时，也因其天生脆弱性而为国家、社会与人的安全酝酿了极大的不稳定性与不确定性，网络安全已成为信息化时代各国的重要议题。对中国而言，网络安全威胁呈现高度复杂性、动态性与模糊性，是当前中国安全领域中极为敏感、脆弱、也极不易掌控的部分，[③] 高层已对网络安全之于国家安全的前提性地位做出了明确判定。[④]“多元性”非传统安全为网络安全分析提供了新的视角，其以“优态共存”为安全治理方略，突破了西方中心主义与“进攻 - 防御”型的网络安全定位，具有更加鲜明的合理性与优越性。从中国对网络安全的定位与规划看，中国网络安全维护需要“多元性”非传统安全的理论指导，在安全价值、安全方略、安全体制、安全政策、安全行为、安全话语、安全研究等多方面加强具体、可操作的能力建设。

【收稿日期：2013-12-31】
【修回日期：2014-03-02】
【责任编辑：齐 琳】

① 董青岭、戴长征：《网络空间威慑：报复是否可行？》，载《世界经济与政治》，2012年第7期，第99-118页。

② 余潇枫：《共享安全：非传统安全研究的中国视域》，载《国际安全研究》，2014年第1期，第3-33页。

③《慎提“网络主权”概念 我国网络安全脆弱》，人民网， http://military.people.com.cn/n/2013/0605/c1011-21748358.html。

④ 2014年2月，中国高层已建立“中央网络安全和信息化领导小组”，并明确提出“没有网络安全，就没有国家安全”以及“建设网络强国”等。新华网：http://news.xinhuanet.com/legal/2014-02/27/c_119538719.htm。

向人回归：中国的“人的安全”路径

任 晓 李燕星

【内容提要】“人的安全”概念强调普通人的安全和福利以及他们作为人的尊严和幸福。它已成为新的研究和政策议程的组成部分。人的安全从出现开始，就在中国学术界得到了讨论，但政府很少使用该术语。就政策领域而言，中国式“人的安全”路径的一个特点就是接受或发展了人的安全的思维并付诸实践，或是殊途同归，但不使用“人的安全”这一特定术语。然而人的安全的本质却反映在中国的内政外交政策中，并且随着国内政策思想而转变为“以人为本”。人的安全已经嵌入中国的安全思维中。作为理解、解释以及更好地分析安全的新视角，引入“人的安全”和“以人为本”是对研究和政策议程的一个积极发展。在中国语境中，尽管“以人为本”的原则并非人的安全最完美的对应物，但它至少表明，当处理国内外与安全相关的事务时，个人安全比过去更加重要了。比起接受“人的安全”这个术语本身，中国更愿意将人民的安全（和幸福）作为政策导向。“以人为本”和人的安全是互相联系和本质一致的。

【关键词】人的安全；以人为本；中国路径

【作者简介】任晓，复旦大学中国外交研究中心主任、教授（上海 邮编：200433）；李燕星，上海浦东图书馆（上海 邮编：201204）。

【中图分类号】D815.5【文献标识码】A【文章编号】2095-574X（2014）03-0040-12

* 衷心感谢《国际安全研究》杂志匿名审稿专家对本文的评审意见，文中疏漏由作者负责。