

网空冲突中的软性竞争

The Friendly Side of Cyber Conflict*

帕纳约提斯·雅纳科乔戈斯博士, 美国空军防务分析员 (Dr. Panayotis A. Yannakogeorgos, Research Professor, USAF)

互联网治理定义宽广, 治理内容包括基础结构、标准化, 以及法律、社会文化、经济和开发等事项。但是, 与互联网关键资源治理及其对美国国家安全的影响相关的思考, 却经常被忽视。美国以外国家试图改变互联网的技术管理和技术标准设计, 长远而论, 他们的行为可能会危害美国国家利益。鉴于目前的互联网治理现状面临诸多全球性挑战, 包括那些意在取而代之的另类计算机网络在网空的崛起, 确实需要集思广益加以应对, 本文探讨美国国家安全政策背景, 并提出软性征服概念和保障信息自由流动的互联网治理多相关方共管格局建议。

互联网治理对美国国家网空战略的意义

技术标准和规范不像那些对国家网空安全的较为明显的威胁那样受到重视。在人力资本和资源受限的环境中, 人们关注的重点是犯罪行为、间谍活动和其他形式的网空冲突, 而不是与互联网关键资源治理、技术标准的制定以及新型电信设备设计有关的事项。一些政策学究们原来谈到网空就发怵, 面对错综复杂的互联网治理, 就更不赞成把资源投入在物理世界找不到类比的这个领域。网空目前处于自由和开放形态, 但是不

ICANN = 互联网名称与数字地址分配机构
ITU = 国际电信联盟

会永远如此。因此, 理解互联网治理的战略层面意义, 和理解攻击者可能如何利用美国的网络漏洞破坏美国国家安全, 两者同样重要。从国家安全角度考虑, 互联网的技术管理很重要, 因为极权国家也许能通过技术手段对互联网的内在基础结构施加威力和影响。而从全球安全角度考虑, 通过互联网治理机构的管理来维护信息自由流动的价值, 将有助于继续推动发达国家及发展中国家促进创造发明和经济繁荣。

美国目前关于国家战略的主要政策文件和论述都主张对网空威胁做出国家反应。¹ 这些战略观点所关注的是灾难性国家安全事件, 而不是设定技术标准或管理互联网日常运行的组织机构之间的纷争。白宫的发言倒是强调了通过现行的多相关方共管平台制定和实施统一技术标准的重要性, 具体提出: “协作开发一致同意的信息和通信技术国际标准……是保障开放性和交互操作性、发展我们的数字化经济、推动社会进步的一个重要方面。”² 此外, 政府也看到了国际标准制定机构面临的挑战, 认为 “在设计下一代标准体系方面, 我们必须以共同利益为重, 支持最合理的技术标准和治理结构, 而不是那些只着眼于提高国家威望或政治控制力的技术标准和治理结构。”³ 但是, 这些考虑被淹没在种种耸人听闻的、臆想的网空末日的讨论之中。

* 此文原刊登在美国空军大学《战略研究季刊》2012年秋季号, 标题为 “Internet Governance and National Security”。本刊请作者对之删减并做适当改动后, 翻译和重新发表, 以飨中文读者。

要保障国家安全，就要求互联网所赖以立足的语言——技术标准和协议——继续保障信息自由流动。如果像某些人所说的，在网空中“编码就是法律”，⁴那么标准和协议就是经脉，使这些编码通过网空现实而获得意义。在政策界，网空已经被视为一块“无形的领域”。因此，技术标准和协议更是加倍的“无形”。然而，这些协议界定着互联网及其关键的基础结构的特征。一如有人指出：“软件和硬件设计所遵循的基本协议代表了制约行为和制定公共政策的一种更加内在和更加无形的体系结构……在这个意义上，协议有其政治赋形——它不是一个虚无的躯壳，而是由协议设计者及实施者演化而成。”⁵过去，美国引领世界制定协议和标准，因此，互联网的设计和特征渗透着自由价值观，孵育了不断推动全球社会经济发展的创新精神。

网空冲突中的软性竞争

有关互联网标准和治理机构的纷争酝酿已久，一触即发，将对未来互联网的特征起决定性影响。俄罗斯和中国部署了先进的IPv6协议，实力相当的其他国家也在制定新的标准，他们都在把新的技术标准推向全球市场，形成网空冲突的软性竞争。

当某个系统的非核心运行者与核心运行者结成伙伴合作关系，藉以取得某个所需信息系统的访问权限时，即发生软性征服。网空理论家马丁·利比奇（Martin Libicki）认为：

控制系统者也许会允许其他人访问该系统，让他们使用其内容、服务和连接。随着时间推移，如果这样的访问很有用……用户也许会逐渐依赖该系统，于是把标准和协议应用于自己的系统，从而加深这种依赖，并投入人力物力，以

便更好地使用他们喜欢的内容、服务或连接。⁶

在这种联盟关系中，核心合作伙伴逐渐处于支配非核心伙伴的地位，后者越来越依赖核心伙伴提供的网络系统服务，连同其漏洞。于是出现担心：“对别人的全面依赖性渗透自己的内部系统，可能使自己受制于别人……系统易受攻击可能有多种原因，例如合作伙伴对网络基础结构的安全性有全面的了解，或者利用对基础结构的访问权限更轻易地启动攻击。”⁷

互联网及其基础技术结构明确地显示了美国作为信息系统的核心运行者，如何通过创建互联网技术和设定其运行规则，软性地支配着盟友和敌邦。互联网依赖美国实体设计及运行的产品，这些实体包括域名系统、互联网名称与数字地址分配机构（ICANN）、微软公司、思科公司，等等。世界各地的用户，例如谷歌和脸书，现在也依赖这个平台上提供的各项服务。然而美国实体目前享有的支配地位不可能永久。爱沙尼亚开发的Skype就是一个例子，说明网络服务并非一定要来自美国。但是，即使某项基于互联网的服务是外国创建的，该项应用程序传送的大部分信息还是要经过位于美国的硬件设备。当发现有网络漏洞时，其他国家也许会尝试退出我们的信息系统，以保护他们自己的网空主权，并且扩大他们的影响力，吸引客户离开互联网，改为使用他们自己创建的系统。⁸因此，美国在网空的战略优势不是无限期的，而且目前正在不同程度上受到实力相当的竞争者的挑战。有鉴于此，我们应该了解其他国家对美国技术优势的反应，从网空软性征服的角度调整我们的网空战略。

软性征服所关注的，并不限于敌方仅能渗透供应链及在对美国国家安全至关重要的

服务器上创建后门程序然后潜入美国信息系统。⁹ 我们面临的威胁还来自国外新技术的出现，而美国并非这些新技术的核心运行者，并且可能会依赖这些新技术。我们关注恶意网空攻击，却没有重视网空世界的柔软腹部——那些使得网空能够从电磁频谱中兴起的技术和标准。

中国正在网空中播撒全球软性征服的种子，且进展神速。根据美中经济与安全评估委员会的报告，“如果照目前的趋势继续发展，就消费、生产和创新而言，中国（及其利益代理人）将在许多领域有效地成为市场主要推动力，其中包括电信领域。”¹⁰ 美国依赖中国制造的计算机芯片和其他信息及通信技术硬件，使得病毒和后门程序能够进入包括军方在内的美国机构和企业所用的设备中。中国制造的计算机硬件的价格异常低廉，畅销于亚洲和发展中国家。¹¹ 此外，在下一代移动式 4G LTE 网络的标准制定方面，中国实体，例如华为，正在引领全世界。¹²

互联网治理与多相关方共管模式

跨国公司等企业实体在国际电信联盟（ITU）内对国际通信监管政策的制定做出直接贡献，并通过其员工在 ICANN、互联网工程任务组和其他组织内做出非直接的个人贡献。

美国政府在 1990 年代出于战略理由禁止出口强化加密软件，但遭到私有企业的反对，最后在这场所谓的加密技术战争中败给后者。也有些公司为了防止犯罪分子使用无法解开的密码进行通信，采用执法部门拦截机制，以便国家安全机构能够监控可疑的犯罪分子和恐怖分子的通信。还有些制定、维护和修订核心标准及基础技术结构的美国公

司和相关个人因为与政府安全部门合作，而遭致贬毁，被指责为私有公司与流氓手法的国家安全机构同流合污，捕获全世界的所有数据。事实并非如此，美国和那些极权国家不同，只要严格认真遵守旨在保护用户隐私的美国法律，就可明确保持政府与私有企业之间的界限。有些媒体为追求轰动效应，动辄刊登这类指责，导致全球对美国私有企业的信任减退，同时为互联网治理机制必须国际化的主张提供了支持。

在美国，电信服务提供商（可追溯到电报系统时代）从来都不是国有垄断体制的一部分，世界其他地区则并非如此。¹³ 例如，英国电信公司和德国电信公司一直都是国有企业，到 1990 年代才转为私营。当然，在美国，电信公司尽管没有国家直接控制，仍接受国家的监管。在国际电信谈判中，国家与各大信息及通信技术公司有一种共生关系。¹⁴ 自 ITU 的前身国际电报联盟在十九世纪中期开始开会监管电信政策以来，始终如此。¹⁵ 因此，发展中国家认为，“由于大部分垄断性互联网公司都是美国公司，目前……美国法律便当仁不让地套用于全球。”¹⁶

那种认为美国政府实际上控制着互联网关键资源的全球通行观点，在很大程度上是因为其他国家的电信公司同其本国政府有密切的关系，于是以为美国也不例外。其实美国的情况很独特，美国政府从来没有拥有或运行任何一家电信公司。随着世界上其他国家向美国电信行业私有化模式转化，过去由政府控制电信行业的经历仍记忆犹新。今天，这些经历给 ICANN 与美国商务部之间签订的特殊协议蒙上了一层怀疑的阴影。

事实上，域名系统最初是由美国国防部发明的，并在其成形阶段由国防部负责技术

管理，然后在 1998 年移交给商务部，后来逐步演变成目前的非政府多相关方共管模式。¹⁷ 这个模式的名称反映了互联网基本技术以及参与制定互联网技术功能标准的组织机构。

互联网关键资源“在互联网治理意义上通常是指互联网独有的逻辑资源，而不是指并非互联网独有的实体基础结构部件或虚拟资源。关键的互联网资源必须提供一个需要中央协调的、具有全球独特性的技术要求：互联网地址、域名系统、自主系统号码。”¹⁸ 一般人认为互联网是无极限的，实际上，基本的地址空间是有限的。事实是，互联网协议地址空间几乎已经用完。工程师们预见到互联网协议的这个问题，研发了 IPv6 协议。它有许多优点，例如，IPv4 的可用 IP 地址数目是 4,294,967,296，而 IPv6 则增加到 2^{128} 。今天，许多人认为：“部署 IPv6 是长期舒缓公共 IPv4 地址库压力的唯一途径……”¹⁹ 在全世界开始采用 IPv6 作为全球互联网主要通信协议，逐步取代 IPv4 之际，美国并未在这方面领先。目前，就市场渗透率而言，俄罗斯的部署范围最广；按数量计算，中国的部署量最大。²⁰ 部署迟缓的后果牵涉到互联网治理和传统型安全威胁。关于后者，美国国家标准局指出：“在 IPv6 部署的最初几年里，防止未获授权而进入 IPv6 网络可能会更加困难。”²¹ 因此，在全国部署 IPv6 方面有较多经验的竞争国家对于该协议在现实世界的运行技术有更多的了解。整个美国空军非保密互联网协议路由器网络在 2014 年之前不会全部使用 IPv6。根据计划，即使到那个时候，也会继续在 10 至 15 年之内同时使用 IPv4 和 IPv6。²² 随着 IPv6 逐渐成为互联网主干协议，俄罗斯和中国也许会被人们理所当然地视为 IPv6 主导国家，而且它们将

会利用这个机会试图把紧缺的地址空间的控制权从 ICANN 转移到某个跨政府机构，例如在联合国架构下的某个机构。

由于网空是一个人造领域，因而其基础结构和标准化非常重要。一些以计算机科学家和工程师为主的全球性组织创建了互联网的运行标准和规则。这些全球性组织中包括前身是美国国防信息系统局、美国国防部高级研究项目局或其他美国政府计划机构、后来在 1990 年代中期实行私有化的那些机构。在下一代互联网的开发中，美国可能不是主要推动国。目前，俄罗斯、中国和其他外国科学家和工程师们正在制定标准和流程。今天的网络设备使用英语作为相互通信语言。如果美国的科学领先地位继续走下坡路，今后的网络也许会依赖讲外语的设备。另外，域名系统和 IP 地址分配的管理也将受到挑战，有些人试图把管理权从目前的多相关方共管平台转移到 ITU 体制内的某个跨政府机构。这就是网空冲突中的软性竞争。

围绕互联网政策的争论证实了多边主义无济于事，因为尽管美国竭力尝试牵头，其他国家并不响应。美国拥有互联网主干结构开发和维护方面的创新技术，这毋庸置疑。但是，世界各国竭力推行监管改革，例如力主让 ITU 之类的全球治理机构监督 ICANN。这已成为一个剑拔弩张的政治问题，与国家网空安全密切相关，对于民主国家和极权国家都是如此。总之，美国在平等国家之间的“领先地位”反而导致争论进入一个又一个的死胡同。我们现在看到，无论是盟友还是竞争对手都在采取反制行动，并且这些行动可能在 2012 年世界国际电信会议期间会加大力度。²³

世界各国对现状的挑战

信息经由互联网等网空开放元实行全球流通,受到相关国家和区域机构的监管,这些机构在国际上相互协调政策。为网空某些组成元制定的标准都经过如国际标准化组织和 ITU 等不同机构的漫长审查流程,是为确保各国之间有充分的技术和政治合作。过去,互联网技术标准由美国实体制定;现在,华为和中兴等中国实体正在互联网治理机构内发挥越来越大的作用,他们参与起草重要的国际标准,将影响世界上下一代网络的架构。这不是最近才发生的事情。早在 2004 年,在 ITU 电信标准化部门担任高级职务的几名中国籍专家就开始谈论利用向 IPv6 协议过渡的机会纠正他们认为美国和发展中世界之间的地址分配不平衡问题。“IPv4 地址的早期分配导致地理区域不平衡,较早采用该协议的国家占有过多的地址空间。区域互联网注册管理机构(RIR)注意到这种情况并采取了一些对策……有些发展中国家对 IP 地址分配提出质疑。重要的是,应确保 IPv6 不会出现类似的问题。”²⁴ 这种情况说明有些国家希望能把 IPv6 地址分配管理转移到 ITU 等全球性机构。

在联合国的政治论坛上,要求改革互联网治理的呼声越来越高。竞争对手和合作伙伴在俄罗斯和中国的带领下,携手要求互联网技术管理国际化。中国和俄罗斯,联合了印度、南非及巴西,带领各国反对美国在 ICANN 中的支配地位。这些活动已经持续了将近十年。²⁵ 随着美国国防部高级研究项目局网络 ARPAnet(互联网前身)实验成功,现已成为全球社会经济发展的一个重要部分,而且各国政府越来越意识到该网络的重要性,要求将网络主干机构 ICANN 国际化的活动力度也越来越大。前面说过,这种国际化呼声

的部分起因是,其他国家因为自己的政府与电信公司在历史上有特殊关系,故而以此类推,认为美国政府也是通过商务部和国家电信与信息管理局控制着 ICANN。

本文认为,由 ITU 控制 IPv6 空间的一个较为可行的方法是,ICANN 向 ITU 提供自己的 IP 地址块,并担任其本身的区域互联网注册管理机构,形成在国家层面分配国家级互联网注册管理机构的做法。这样做既可以保持目前管辖互联网关键资源的多相关方共管框架,同时又能充分照顾到中国和发展中世界的需求。它可减少摩擦,并且让喜欢现行模式者能继续使用该模式监管互联网的日常工作。

在信息社会世界首脑会议(W SIS)筹备阶段,对现有互联网治理体制的强烈反对声浪开始涌现,使会议成为关于 ICANN 国际化争论的一个战场。例如,在 2004 年 3 月联合国主持召开的全球互联网治理论坛上,²⁶ 巴西代表玛丽亚·路易泽·维沃提声称互联网治理需要改革,因为它没有包括发展中国家,而且似乎被某些国家或利益相关方所霸占。²⁷ 南非全国委员会主席琳达·肖普-马弗尔也持类似的观点,认为发展中国家最担忧的是 ICANN 流程的合法性,而不是其功能运作。²⁸ 于是,与会代表经过认真讨论,根据发展中国家提出的关注事项,最终同意 ICANN 需要进一步改革。在整个 WSIS 会议期间,以及随后召开的讨论互联网治理和全球网空安全的其他会议上,巴西始终强烈反对美国在 ICANN 的支配地位。2011 年,印度声援南非和巴西,建议“具体落实突尼斯指令”,其建议内容为:

鉴于对透明、民主和多边机制之需要,以便所有的利益相关方能发挥各自的作用,处理需要引起关注但现有机制未能

妥善处理的许多跨国国际公共政策问题，并鉴于对加强合作之需要，以便各国政府能在平等的基础上履行与互联网相关的国际公共政策领域的各自义务和责任，印度建议在联合国建立一个新的主管全球互联网相关政策的机构，该机构可称为联合国互联网相关政策委员会（CIRP）。²⁹

成立互联网相关政策委员会的建议被视为对目前互联网技术管理的反制手段，在发展中世界获得很大反响。实际上，这个建议在很大程度上反映了中国政务和公益机构域名注册管理中心（CONAC）所表达的中国观点，该中心认为“美国政府掌握了互联网资源的控制权。因此，我们建议应该使所有的多相关方都能够对计算机安全计划发表意见，因为维护网空安全不是美国政府单方面的使命，也没有任何一个国家能够单独完成这项使命。”³⁰

俄罗斯前总理普京也表示：ITU 是年代最久远的国际组织之一；它的历史比联合国还长出一倍。俄罗斯是其共同创建国之一，愿意成为一个积极的成员。我们感谢各位提出的各种讨论议题。其中一个是利用 ITU 的监控和监督能力对互联网实行国际监管。³¹

因此，美国在 ITU 内面临着来自极权国家带领的发展中世界的严重挑战，他们要求把互联网关键资源的控制移交给一个多边机构。这个要求内含的基本危险是，具有信息自由流动关键特征的互联网将演变到听任非民主国家的政治日程控制信息流动的模式。因此，美国以及观念相同的其他国家必须在外交上挺身而出，确保互联网保持信息自由流动的特性，避免受到多边机构的政治控制。

围绕互联网控制权的外交斗争在其他各种论坛上也有发生，例如联合国科技发展委员会。人们提出了许多建议，包括：

建立一个隶属于科技发展委员会的临时工作组，在联合国秘书长的支持下制定机构设计和路线图，以便在互联网相关公共政策问题上加强合作……

在联合国系统内建立一个较永久的互联网相关国际公共政策问题委员会，可以参照经济合作与发展组织信息、通信与计算机政策委员会的模式……

更具体的是，全球政策问题应该由一个具有全球代表性的机构来处理，例如联合国；而区域问题则应该由具有区域代表性的机构来处理，例如欧盟委员会……[而且] 相关组织应该参与每四年举行一次的 ITU 全权委员会关于互联网治理的讨论，以及 ICANN 的公共审议流程和政府顾问委员会讨论。³²

鉴于世界电信会议将在 2012 年 12 月召开，上述言论表明人们会再次提出这些主张，要求 ITU 修订《国际电信条例》，把对下一代互联网关键资源的管理包括在 ITU 条例内，推动此国际机构在互联网治理方面发挥更大的作用。³³

让互联网治理向跨政府流程开放，可能给全球经济安全带来风险，因为责任心不强的国家也许会对互联网治理采取目前私有化放任自流的态度，并且让国家和国内公司实体控制互联网关键资源的管理。

影子域名系统的崛起

互联网关键资源之所以能保障普遍可解析的 URL 地址和全球互联网通信，应归功于 ICANN 管理的根系统以及互联网工程任务组

(和其他机构) 内部设计、开发和论证的各种协议。尽管这个流程可确保自由和开放的互联网运行, ICANN 用于维护域名注册管理机构的标准和协议也可被个人、临时网络和某些国家用来设计及部署自己的另类域名系统, 这些替代系统可以独立于互联网或“搭载”于互联网之上。公司的局域网 (LAN), 例如公司内部使用的“.company name”网络, 就是独立于互联网的网络。当某个组织想要搭载于全球域名系统根名之上, 并把自己的伪顶级域置入其中时, 伪域的核心运行者可以使用特定的软件资源在其替换域名系统内解析全球可用的域名。美国浏览用户可以通过洋葱路由器 (TOR) 网络进入另类域名系统, 获得亲自感受。用户可以下载洋葱路由器套装软件, 导航到想要匿名访问的网站 (这是 TOR 的典型用途), 用 TOR 浏览器指向“.onion”域上的相关网站, 进入网空地下社会; 在这片空间中, 业务运作管理已经开始躲闪转移, 目的就是摆脱执法机构的监视, 为自己的真实身份再加一层保护。

如果大量使用这类影子互联网, 可能导致人们对互联网的信心减弱, 其使用量也会下降。最大的风险是, 当某些国家开发和部署供其自己内部使用的另类域名系统时, 他们会与全球互联网隔离。这种情况不同于控制进入点和实际开发国家级内联网且自行作主是否接入全球互联网的做法。³⁴ 俄罗斯和中国在部署供国内使用的潜在的新内联网方面已经有所作为, 伊朗等其他国家也在学样。

美国参与公开倡导和组织“数字活动分子”(digital activists), 为确保信息自由流通而斗争, 结果造成国际摩擦; 美国调拨高达三千万美元的资金, 用于提升互联网的开放式访问性能, 支持数字活动分子, 并反击任何国家对互联网的压制。³⁵ 这么做对于促进

网空安全问题的国际合作并无助益。“互联网自由议程”就是这种情况的一个例子。³⁶ 此类技术使得公民活动分子能够有效地绕过政府的系统监控工具, 传播被禁止的信息。还有一些其他工具, 使得活动分子能够披上数字伪装, 组织以推翻现有政权为目的的社会运动。结果是, 导致产生了另类国家网络, 创建了供国内使用的另类域名系统, 使得执政当局能够审查网络内容和抑制现有互联网结构所促进的生产率。中国已经在国家范围内做到了这一点。在国务院国有企业改革办公室以及工业和信息化部授权下, 中国政务和公益机构域名注册管理中心管理“.政务.cn”和“.公益.cn”两类国内网站的域名注册。

分裂性互联网的崛起肯定会改变现有互联网的特征, 对全世界的创新和繁荣造成负面影响。那些希望互联网保持自由和开放特征的人们将受益于自由和开放, 并且与那些企图控制互联网一个总开关的人形成显著的道德对比。因此, 维持现有的互联网治理模式, 同时妥善处理友方和盟国的合理疑虑, 将有助于确保互联网继续发挥人类经济发展的稳健平台的作用。

结语

如果不重视我们在互联网治理方面的漏洞和软性征服, 可能使我们的敌人在网空冲突中获得战略优势, 并使我们自己的网空攻击行动变得更复杂, 因为我们的竞争对手正在部署以非美国实体开发的协议和标准为基础的网络。我们必须就这些问题开展广泛的对话, 以加深对网空的了解, 并且适应网空环境中发生的变化。尽管在历史上互联网起源于美国国防部, 但是美国从来没有很好地组织人力去影响与互联网治理有关的技术标

准和政策的制定。目前，国防部依然采取被动响应态度，只是协调和评论美国政府流程中正在考虑的与互联网治理有关的各种全球规范和标准。由于这种被动态度，国防部和美国空军可能被外界视为不具备互联网治理的法律知识或技术资历。国防部，尤其是美国空军，应该像以前一样发扬领导责任，在信息技术基础结构标准的制定方面发挥更积极的作用。此外，国防部应该更加仔细地制定书面政策，界定其作用，系统地指引自己如何参与互联网治理机构的活动和其在其中的地位。空军应该在国防部和整个政府体制内起到带头作用，软性征服概念已经隐含在空军的政策、战略和作战准则之中，现在空军需要更明确地重视更广义的软性征服概念。将于 2012 年 12 月举行的世界电信会议也许可以成为开始这项努力的一个合适场所。

随着作为全球互联网基础的硬件和软件不断演变，以及非美国实体开始研发新硬件、标准和协议，美国实体的市场占有率有可能

被挤占，美国的网空基础结构核心运行者地位将会削弱。目前，美国凭借 ICANN 和顶级域名系统，占据着互联网服务开发者和核心提供者的地位，拥有技术支配权。但是，我们的国家网空安全战略没有充分正视其他国家通过开发将成为下一代网络基础的协议、标准和技术所构成的威胁。美国空军拥有大量的科学家和工程师等优秀技术人才，可以发挥关键作用。但是，它不能单独行动，而国防部则需要从已经有限的网空资源中调拨一部分到互联网治理。如果不这样做，国外设计的技术标准和协议可能会构成下一代信息技术的主干，也许会逆转国防部目前所依赖的互联网信息自由流动的特征，使国防部的作战行动遭遇风险。美国空军始终是对网空最有影响力的美国军种，因此空军在互联网治理争论中的作为或不作为有举足轻重的意义。♣

注释：

1. The National Strategy to Secure Cyberspace (NSSC) [国家网空安全战略], (Washington: The White House, y 2003); 另参看 John Rollins and Anna C. Henning, Comprehensive National Cybersecurity Initiative (CNCI) [全面的国家网空安全计划], (Washington: Congressional Research Service, 10 March 2009; declassified in March 2010); 另参看 International Strategy for Cyberspace [网空国际战略], (Washington: The White House, May 2011); 另参看 the Department of Defense Strategy for Operating in Cyberspace [国防部网空作战战略], (Washington: DoD, July 2011). 这些文件是迄今关于网空安全的最主要的指导文件。
2. 见注释 1 中“网空国际战略”，第 12 页。
3. 见注释 1 中“网空国际战略”，第 15 页。
4. Lawrence Lessing, “Code is Law” [编码就是法律], 见 Code: And Other Laws of Cyberspace, Version 2.0 [编码：以及其他网空定律，2.0 版], (New York: Basic Books, 2006), 11-10.
5. Laura DeNardis, Protocol Politics: The Globalization of Internet Governance [协议政治：互联网治理的全球化], (Cambridge: MIT Press 2009), 11.
6. Martin Libicki, Conquest in Cyberspace [网空征服], (New York: Cambridge University Press, 2007), 12.
7. 同上，第 137 页。
8. 全球定位系统（GPS）是争夺软件和硬件控制权的一个例子。尽管使用 GPS 的基本服务是免费的，友方和竞争对手都意识到他们对这套美国系统的依赖性使他们易于陷入受人摆布的境地。俄罗斯正在革新其 GPS 系统，欧盟和中国则在自行开发独立的 GPS 系统。这些新系统从意图形成到具体落实有一个很长的时间周期，因为部署一个太

- 空网络涉及巨额投资。网空系统的时间周期可能短一些，因为与发射多个高科技卫星到太空相比，部署一个国家级计算机网络的成本较低。关于另类 GPS 系统的详细论述，请参看 Lt Col Scott W. Beidleman, GPS versus Galileo: Balancing for Position in Space [GPS 与伽利略卫星导航系统：空间定位竞技], (Maxwell AFB, AL: Air University Press, 2006).
9. Bruce Rayner, "Ferretting out the Fakes" [揪出赝品], *Electronic Engineering Times*, 15 August 2011, 24; 另参看 John Markoff, "Computer Gear may Pose Trojan Horse Threat to Pentagon" [计算机零部件可能给五角大楼带来木马病毒威胁], *New York Times*, 10 May 2008, 12.
 10. The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector [美国电信行业中来自中国的投资和产品对国家安全的影响], U.S.-China Economic and Security Review Commission Staff Report, January 2011, 7, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.
 11. LCDR A. Anand, "Threats to India's Information Environment" [印度信息环境面临的威胁], 见 *Information Technology: The Future Warfare Weapon* [信息技术：未来战争的武器], (New Delhi: Ocean Books Pvt. Ltd., 2000), 56-62.
 12. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial" [华为进行世界上首次商业网络 LTE Category 4 测试], *Cellular News*, 9 May 2012, <http://www.cellular-news.com/story/54329.php>.
 13. Anton A Huurdeman, *The Worldwide History of Telecommunications* [世界电信史], (Hoboken, NJ: John Wiley & Sons, 2003), 91-146, 153-85; 另参看 Jill Hills, "International Market Structure and the ITU" [国际市场结构和国际电信联盟], 见 *Telecommunications and Empire* [电信与帝国], (Champaign: University of Illinois Press, 2007) 91-116.
 14. Edward Comor, "Communication Technology and International Capitalism: The Case of DBS and US Foreign Policy" [通信技术和国际资本主义：DBS 和美国外交政策案例研究], 见 *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy* [全球通信政治经济学：霸权、电信和信息经济], ed. Comor (New York: St Martin's Press, 1994), 83-102.
 15. Jill Hills, *The Struggle for Control of Global Communications: The Formative Century* [争夺全球通信控制权：格局形成的世纪], (Champaign: University of Illinois Press, 2002.)
 16. Parminder Jeet Singh, "India's Proposal Will Help Take the Web out of U.S. Control" [印度的建议有助于使互联网摆脱美国的控制], *Hindu Online*, 17 May 2012, <http://www.thehindu.com/opinion/op-ed/article3426292.ece>.
 17. Department of Commerce, *Management of Internet Names and Addresses* [互联网名称和地址的管理], 63 Fed. Reg. 31741 (1998).
 18. 见注释 5 中“协议政治”，第 11 页。
 19. M. Ford, M. Boucadair, A. Durand, P. Roberts Issues with IP Address Sharing [IP 地址共享问题], (Internet Engineering Task Force, RFC 6269) June 2011 <http://www.hjp.at/doc/rfc/rfc6269.html>
 20. Ingrid Marson, "China launches largest IPv6 network" [中国开始筹建最大的 IPv6 网络], *CNET News*, 29 December 2004, http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html.
 21. Sheila Frankel et al., *Guidelines for the Secure Deployment of IPv6* [安全部署 IPv6 指南], (Gaithersburg, MD: National Institute of Standards, December 2010).
 22. Katherine Kebisek, "AFNIC prepares Air Force for IPv6 transition" [空军网络整合中心准备协助空军过渡到 IPv6], *Air Force Space Command* (4 April 2011), <http://www.afspc.af.mil/news1/story.asp?id=123249968>
 23. 关于互联网治理的争论已有大约十年的历史，肯定将持续到 2012 年以后的年份。信息社会世界首脑会议的下次聚会将在 2015 年。
 24. H. Zhao, "ITU and Internet Governance—input to the 7th meeting of the ITU Council Working Group on WSIS, 12-14 December 2004" [国际电信联盟和互联网治理——提请 2004 年 12 月 12-14 日召开的国际电信联盟委员会信息社会世界首脑会议工作组第 7 次会议考虑的几点意见], www.itu.int/ITU-T/itsb-director/itut-wsis/files/zhao-netgov02.doc.
 25. Panayotis A. Yannakogeorgos, "Cyberspace: The New Frontier and the Same Old Multilateralism" [网空：新疆域和旧多边主义], 见 *Global Norms, American Sponsorship, and the Emerging Pattern of World Politics* [全球规范、美国赞助和世界政治的新兴模式], ed. Simon Reich (New York: Palgrave, 2010).

26. “UN ICT Task Force Global Forum on Internet Governance to be Held in March” [联合国信息及通信技术任务组互联网治理全球论坛将于 3 月召开], UN press release, Paris, 13 February 2004, http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html.
27. “Global Internet Governance System is Working But Needs to Be More Inclusive, UN Forum on Internet Governance Told” [联合国互联网治理论坛被告知, 全球互联网治理系统在发挥作用, 但需要有更大的包容性], UN press release, 26 March 2004, <http://www.un.org/News/Press/docs/2004/pi1568.doc.htm>.
28. 同上。
29. “Statement by Mr. Dushyant Singh, Member of Parliament, on Agenda Item 16—Information and Communication Technologies for Development, at the 66th Session of the United Nations General Assembly on October 26, 2011” [Mr. Dushyant Singh 在第 66 届联合国大会 2011 年 10 月 26 日全体会议上就议程第 16 项“信息和通信技术的发展”发表的讲话], <http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html>.
30. Yang Yu, Chinese response to “Further Notice of Inquiry on the Internet Assigned Numbers Authority Functions” [中国对“关于互联网号码分配机构功能质询的进一步通知”的反应], China Organizational Name Administration Center (CONAC), http://www.ntia.doc.gov/files/ntia/conac_response_to_fnoi.pdf.
31. “Prime Minister Vladimir Putin meets with Secretary General of the International Telecommunication Union Hamadoun Toure” [普京总理会见国际电信联盟秘书长哈马顿·杜雷], Working Day, 15 June 2011, <http://premier.gov.ru/eng/events/news/15601/>.
32. UN General Assembly, “Enhanced Cooperation on Public Policy Issues Pertaining to the Internet” [在互联网相关的公共政策问题方面加强合作], Report of the Secretary-General, http://unctad.org/meetings/en/SessionalDocuments/a66d77_en.pdf.
33. 国际电信条例 (ITR) 有 178 个签约国, 是一个全球适用的条约。
34. 这不同于 Chris Demchak 在 “Rise of a Cybered Westphalian Age” [网空威斯特伐利亚和约时代的到来] 中所指的情况, 此文见 Strategic Studies Quarterly 5, no. 1 (Spring 2011): 32-61.
35. US Department of State, Internet Freedom Fact Sheet [互联网自由简介], (15 February 2011) <http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm>
36. Spencer Ackerman, “Does Obama’s ‘Net Freedom Agenda’ Hurt the U.S.?” [奥巴马的“网络自由议程”伤害美国吗?], Wired, 28 January 2011, <http://www.wired.com/dangerroom/2011/01/does-obamas-internet-freedom-agenda-hurt-the-u-s-without-helping-dissidents/>.



帕诺·雅纳科乔戈斯博士 (Dr. Pano Yannakogeorgos) 是美国空军大学空军研究所的网空政策与全球事务研究教授, 其研究领域包括网空与全球安全交汇、网空规范、网空武器控制、非国家暴力行为体, 以及东地中海研究。他曾是罗格斯大学 (Rutgers University) 全球事务中心资深项目协调员, 并曾担任联合国安全理事会顾问。他拥有罗格斯大学全球事务硕士和博士学位, 以及哈佛大学文科学士学位。