免责声明：凡在本杂志发表的文章只代表作者观点，而非美国国防部、空军部、空军教育和训练司令部、空军大学或美国其他任何政府机构的官方立场。

来自网空用于网空：明确网空情监侦作战的概念

For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance

作者：美国空军上校马修·M·赫尔利（Col Matthew M. Hurley, USAF）

二十年以前，即在数码时代的初晨，我们还只能从科幻作品中看到人类在某种合成的、虚拟的领域中交往和争斗。[1] 我们曾被《创战记》和《战争游戏》等科幻电影刺激得激动不已，一想到《终结者》中的“天网”将可能如电影预示的那样具有自我意识就不寒而栗。然而，电影一结束，我们便揉去眼前的噩梦，重新步入光明的“真实”世界。

曾几何时，今天的我们已经不再把网空视为科幻的异想天开，而是一个与陆、海、空、天这四个传统环境同样重要的作战领域。[2] 当然，网空与这四个我们较熟悉的自然领域又有显然的不同。情报 / 监视 / 侦察（ISR—情监侦）作战如何在这个新的、变幻无穷的人造环境中运作和发挥？美国空军情监侦部门在努力认识这个新奇作战领域的过程中正面临那些挑战？以及，空军情监侦部门应如何应对网空与生俱来的问题和需求？本文将逐次讨论这几个根本问题。[3]

界定网空情监侦

与在自然领域中开展情监侦作战不同，网空情监侦作战还有待在联合或军种作战准则中被正式界定。尽管人们广泛谈及“网空情报”（CYBINT）及其与信号情报及公开源情报的关系、甚至有人呼吁更细地划分为如“SkypeINT”或“VoIPINT”等基于载体的不同情报分类，其实对这个主题，当前的理解仍未成熟。[4] 正如负责情监侦作战的空军副参谋长拉利·D·詹姆斯（Larry D. James）中将在 2011 年所言：“我们才刚刚开始从空军的角度来思考这些事情。”[5] 因此，虽然“网空情监侦”这一术语在空军情监侦部门已经获得了越来越多的认可，它同时也引起了国防部其它部门和空军参谋部对其含义的质疑。[6] 本文首先提供一个概念作为讨论的起点，以助澄清和完善未来的作战准则。

为正确理解网空情监侦作战，也许我们可以将网空活动分为两个行动范畴：来自网

空的情监侦和用于网空的情监侦。来自网空的情监侦可追溯到二十世纪八十年代那些设法从对手网络获取数据的最初努力，今天的分析员继续在网空搜索，梳理出詹姆斯中将所说的“从该领域搜集的任何有情报价值的信息。”[7] 搜索的对象包括比如外国的新闻媒体、威胁行动者经常出没的聊天室、出自危机地区的网络日志和录像或商业图像，等等。它也包含我们较熟悉的计算机网络利用（CNE）这一概念。从网空收集到这些信息之后，我们就能利用它来支持任何领域的作战行动。

就这一点而言，空军政策指令 10-17《网空作战》也许对网空情监侦给出最佳定义。它指示空军情监侦部门的任务是：“确保具备提供协同分析、融合情报、跨域化 / 一体化 / 自动化情监侦 PCPAD（PCPAD 是规划与收集、搜集、处理与利用、分析与生产、分发的英语首字母缩写）的能力，以开展网空作战。”[8] 这个定义揭示了全源情报在网空作战行动的规划和执行期间的重要性。在网空作战，需要的不仅是来自网空的情监侦；任何情报渠道都能为网空行动提供有关键情报价值的信息。[9] 空军情监侦局局长罗伯特·P·奥托（Robert P. Otto）少将指出：“当我们说‘用于网空的情监侦’时，我们指的是为支援网空优势而开展的情监侦作战”——无论什么来源、方法或媒介。[10]

有些人错误地把 CNE 和网空情监侦看成为同一码事，但 CNE 恰好属于第一个行动范围，即来自网空的情监侦。空军作战准则界定 CNE 为“通过使用计算机网络，从目标或对手的自动化信息系统或网络收集数据，从而保障我方的行动和情报搜集能力。”[11] 更明确地说，CNE 的“操作一般是通过网络工具潜入对手的网络系统……操作 CNE 的工具和进行计算机攻击使用的工具相似，但前者是为了情报搜集而不是系统破坏。”[12] 这两种描述都暗示蓄意入侵对手的硬件、软件或相关网络系统。[13] 然而，它们不包括被动搜集有潜在情报价值的公开来源信息。这种被动的情报搜集也是“来自网空的情监侦”的另一个重要形式，包括下载公开发布的敌方最新战斗机的录像，研读外国作战准则或军事出版物，监视聊天室，以及众多在网络系统或网上来无影去无踪的其他活动。它们都有助于达到情监侦的重要目的，即在适当的时候为适当的决策者获取适当的信息。

网络态势感知是一些相关文献中突出描述的另一个与情监侦有关的概念，涉及到察觉、识别并了解网空存在和出现的友善的、敌对的、或介于两者之间的人和事。[14] 然而，态势感知显然不限于情监侦，它还涉及指挥与控制、作战空间感知的非情监侦部分，甚至还有个体认知。[15] 所以，尽管情监侦是态势感知的核心部分，但此两者不应该混为一谈。比如，我们不认为环境监测属于情报搜集范畴，虽然它是作战空间感知的一项职能，也涉及到类似的分析过程。我们也不把所有人类知识算作“有情报价值的信息”，即便知识就意味着感知。

有了这个界定和限制网空情监侦的起始点，那么我们就必须探索我们在其中进行情监侦的环境。如下列几段论述所示，网空作为一个领域引起了重大问题，如果我们想充分了解网空，并在其中有效地作战，我们就必须解决这些问题。

网空的挑战

美国兰德公司分析专家马丁·利比奇（Martin Libicki）对美国政治和战略思维的惯

性做出了这样的概括：每当新的趋势（比如一战期间空中作战兴起，太空技术用于军事应用，等等）出现，每当可能改变游戏规则的革新发生，我们最初的反应通常都是削革新之足适成规之履。而今我们已经将网空宣称为一个作战领域，利比奇担心“我们会拿旧尺子来丈量新事物。”他警告说：“但是你不能如此对待网空，你必须根据它［自己］的法则来思考它。”[16] 当然，在所有作战领域，情监侦及其他军事活动中都存在着一些普遍和持久的共性，但是，利比奇的基本观点值得我们注意，即我们不能只是照搬现行的作战准则和战术 / 战技 / 战规，把所有出现“天空”或“太空”的地方改成“网空”就了事。网空有其独特的性质，由此带来新机遇和新挑战，要求我们创新思考，开拓新路，而不是拿旧瓶子装新酒。[17]

网空这个最新作战环境正是以其独特属性，把网空情监侦和“自然”领域里的互补性活动区别开来。首要的、也是最显著的一点是：网空是由人类创建的，人类又在不断地修改它；20 多亿用户的每一次网上点击或键击都波及整个网空。前国家安全局局长及中央情报局局长、美国空军退役上将迈克尔·V·海登（Michael V. Hayden）说：“其它领域是自然的，但网空这个领域是人类的创作。人类能真实改变其地理，网空发生的‘任何事’能在某个人的‘物理空间’产生变化。”[18] 网空既来自人造，便导致了三个特征：复杂性、适变性和变化速度，这三个特征使网空与相对稳定的自然领域有了区别。姑且承认，自然界也是复杂的，随改的，变化的，但是它的变化程度和速度都不能和网空相提并论。我们仍然能认出我们祖先就熟知的那些高山、大海和星辰。然而今日的网空与区区二十年（大致为一个人的兵龄）前的网空已然是天壤之别。[19]

谈到复杂性，网空错综得令人窒息，曲折得令人发狂，一切都彼此相连，现今已生产出 500 亿个装置连在网中，任牵一发即可动全身，效应之深之广，全然不成比例。[20] 因此，网空思维“必须要考虑互联关系，即网络，以及人类是如何构建和使用网空领域的”。网络的海量性、不稳定性、不可预测性、关系复杂性等等，都使得网空思维极难把握和适应。[21]

网空固有的适变性促成了它的复杂性和动态多变性。[22] 它随着网空内外条件（诸如新技术、威胁、政治与法律）的演进而持续不断地（通过数亿个分散用户的行动）变化着。请注意，因特网本身的设计就是为了促进科技发明的飞速扩张和对技术革新的适应。[23] 这些变化既培育了网空的适变性，变化本身也以飞快的速度发生，伴随各种创新的、常常出乎意料的技术不停地改变着网空景观，其改变之快，为其他任何技术领域所不及。[24] 一个四人组英国观察家这样描述说：“变化速度如此迅猛，致使战略演进的传统性行动 / 反应周期还未及开始就已经过时，就好比政府派一位作战分析家去观察燧发步枪交战的效果，当他到达时却发现马克沁机枪都已经发明出来了。”[25]

网空的急剧膨胀进一步加大了它的复杂性和适变性。物理领域的规模大小相对稳定，网空则不同，它在各重大方面都呈几何级数扩张。[26] 到 2011 年中期，人类在网空中已进行了 2 万多亿项交易，涉及到 50 万亿吉字节数据。[27] 让时光快进到 2025 年，我们预期到那时将有约 55 亿数字化居民，代表 60% 的世界预计人口，他们每天将使用 2500 万

个应用程序来进行数十亿项交易，每日生成或交换 50 万亿吉字节数据。网民将有大约 30 亿个因特网主机供其选择，每个主机都可能拥有数千个体网站。[28] 人们苦于想把网空梳理清楚，但它的飞速扩张令人难以招架。

传统上，军事策划者和实践者一直认为，规模大小和距离远近与所需时间成比例关系：穿越远距离或征服大面积都需要更多时间。比如二战期间，护航船队从美国航行到英国用了一周多时间，同盟国从登陆诺曼底到渡过莱茵河就用了将近 10 个月时间。然而，军事上传统的时间概念对网空毫不相干。[29] 理论上，普通人一眨眼的功夫，我们就能把一个数据包从起源地投送到目的地，从地球上的任何一点到任何另一点。网空是以“字节速度”行动。[30]

网空蔓延到全世界每个角落，加之网络效应的速度，它为美国空军的“全球到达”观念增添了一个新的、令人敬畏的维度。[31] 网空物理节点遍布每一个自然领域——五洲四海之内、之上、之周围。网空在全球纵横交错，把人与人之间的距离拉近到前所未见，同时也使敌人有了以往无法想像的攻击便利。[32] 过去，作战人员总是有独立的战区来开展行动。[33] 然而在网空，毫不夸张地说，敌对行动可以发起于或途经任何有因特网设备功能的地点。[34] 而且，网空的全球性质已经使主权实体之间的传统边界基本上失去意义。[35] 由于高超的对手有能力从多处前线进行干扰或袭击而几乎不受惩罚，“地理位置就毫不相干了。因此，判定某个服务器的地理位置根本无济于事，就算知道了某个拒绝服务攻击来自某地点某服务器也说明不了问题，因为攻击者可以利用设在美国的服务器，也可以利用设在中国、马来西亚或者文莱的服务器。容易得很，小菜一碟。”[36] 网空的全球弥散性和地理模糊性对有效开展情监侦增加了复杂性，因为你无法锁定任何静止的物理空间——这从根本上背离了情监侦的地球中心说概念。

不仅主权国家边境，而且主权国家本身，在网空中都开始失去意义。没有哪个网络化的国家政府敢声称对这个领域的力量垄断，也不敢断言完全拥有军事行动所必须的基础设施。[37] 这第一种情况是因为：进入网空成本很低，加上越来越先进的威胁软件唾手可得，使非国家行为体、甚至某些个人，都有机会进行那些以前纯属国家安全机构职责的活动。[38] 但是现在在网空，参与者“不需要受良好教育，也不必拥有充分资源……只需要有破坏意图和技术能力，就能进行破坏活动。”[39] 另外，大约 90% 的网空基础设施属私人所有，尽管它最初可能是由政府资助的，尽管政府和武装部队现在严重依赖这些商业基础设施。[40] 其结果，在网空“公与私、政府与商业、军事与非军事之间的区别和划分，都已模糊不清。”[41]

网空的这些特征帮助造成了令所有情监侦专业人士“最棘手的问题”：如何判定和追溯攻击源。[42] 空军太空司令部承认：“真实（最初）攻击源的隐蔽性使人难以找到攻击者，而且，因特网本身的结构设计就有助于匿名。”[43] 网络参与者的海量人数，也使追踪溯源更加困难，国防部在企图找出一个内部威胁时就遭遇这种困难。如果每个用户代表一个节点，每封电子邮件代表一个链接，在单独一年之内，我们就得分析 237,387,616 节点之间的 755,230,064,000 个链接——这个计数还不包括网络搜索、文件存取，或其它类型的理论上可以观察到的网络活动。[44]

不单潜在目标群规模庞大，网络工具也使追踪溯源进一步复杂化。拥有多达数百万台机器的僵尸网络、专门用于匿名化的代理网站、洋葱路由、以及相关技术等，都为积极判定攻击源设置了令人生畏的障碍。[45] 从根本上说，因特网“天生就是依据未经验证的数据交换协议运作的，”也就是说，“溯源和不可否定性常常与匿名性相冲突。”[46] 追踪溯源虽然极为不易，但也“并非不可能”，第659情监侦大队的指挥官丹尼尔·辛普森（Daniel Simpson）上校如是说；“然而，你需要精明能干的情监侦专业人士进行认真努力的分析。”[47] 尽管在溯源技术有所改进，但如前国防部副部长威廉·J·林三世（William J. Lynn III）说，“总的趋势是越来越困难。来袭导弹回路可知，网络袭击则来路不明。”[48]

攻击源的判定如果不完整或不准确，也有可能导致情监侦部门违反法律、政策和宪法规定。对攻击来源和性质(来自本国或外国，属于犯罪、军事、或情报行动性质）的不确定性，不仅会延误溯源过程，并使我们难以把握美国法典 10/18/50 卷所赋权利；而且不确切或无把握的溯源还可能导致违反这些权利的行为。[49] 如前联邦调查局局长罗伯特·缪勒(Robert Mueller)在听证会上所言:“一开始，你不知道［网空侵入者］是一个国家行为体，还是一帮受国家行为体操纵的个人，或者就是街对面的一个稚气未脱的高中生。”[50] 为应对这一挑战，有人提出了一些方案，比如：军界、情报界、工业界之间共享数据；或者为能积极防御而更大胆和全面地搜集情报；或者“重新设计”因特网以有利于追踪和判定地理位置，等等。但这些提议惹恼了那些主张网上隐私、公民自由、互联网自由的组织。[51] 本文不打算从法律层面开展讨论。[52] 但需要指出：因为有时情报活动和网空执法活动之间的界限不明确，我们可能会面临“陷入网络法律这个未知水域”的风险。[53]

前景与建议

面对网空固有的障碍，如果情监侦部门计划希望在这个最新领域有效地作战，它就必须在思想、资源、人员等方面做出并保持适当的投资。在思想领域，其首要任务是，必须明确情监侦如何参与更大范围的网络作战。目前，空军和联合部队在这一点上缺少共识。大多数军事与国家作战准则及政策文件都着重论述进攻和防御性网空活动，而把情监侦降级为支援角色。例如在 2010 年，空军太空司令部——空军网空作战核心功能的首要协调机构——把情监侦描述为网空支援、网空防御、网空兵力应用等使命所需的一种“能力”。[54]

这些观念都没有认识到，情监侦本身就是一项作战使命。在网空作战过程中的其它任何时候，它始终既是中心又是根本。的确，网空行动“浸泡在情报中”，一旦没有情监侦，网空行动“简直就是俗话说的黑灯瞎火乱开枪。”[55] 詹姆斯中将主张“我们不把情监侦和空天领域的行动分开。在网空，它们甚至连结得更加密切。”[56] 所以，我们需要在作战准则、教育和组织结构等各方面大力强调网空情监侦的核心作用和作战性质——不是为它自身的缘故，而是为了认识到这一事实：假如没有情监侦，我们就将耳聋目瞎，所有行动都将受到损害。

然而为了发挥效力，网空情监侦需要的远远不只是从制度上重视及调拨资金或人力，还必须调整自身适应作战环境。就网空而言，情监侦必须保持全球感知，时刻警戒，预测而不是反应，敏捷主动，并能应对和管理急

剧增长的海量数据。这种愿景进一步要求我们加强招聘和训练网空情监侦专业人才，通过他们更好地保护公民自由和隐私，并且更合理地将网空情监侦融入整个情报界。

建设预测性情监侦和早期预警能力

前国家情报总监迈克·麦康纳（Mike McConnell）等观察家认为，网空情监侦与国防目前的“最新技术水平”只能做到依赖“事发之后的调查取证”来评估损伤和查找攻击发起者。[57] 过去，我们也曾依赖周边防御和防火墙；但是狡猾的敌人总能找到途径绕开或突破无论有多么复杂的“网络马奇诺防线”。[58] 因此，我们需要构建一道“网络远程早期预警线”，应具备溯源和防御能力，能在敌人实施破坏之前就对威胁做出响应。[59]

为对任何瞬间可能发生的攻击做出尽早的预警，我们必须实时感知全球网络活动及其发生背景，以采取更有预测性的措施。[60] 预测性网空情监侦立足于以往经验和对当前趋势的把握，积极查找网空可能发生的破坏活动的任何迹象，诸如某些组织对美国的积怨、“爱国黑客”群体的异常动态、网聊者、新技术、对手的作战准则，等等。[61] 我们必须监视所有这些潜在线索，“不间断地进行，抓住蛛丝马迹顺藤摸瓜，从而做到防患于未然。”[62]

敏捷主动

当然，“早期”预警是相对的。冷战时期我们认为，洲际弹道导弹从发射到落地需要 30 来分钟；但是，如今的网络袭击能在 30 毫秒内从北京闪击纽约。[63] 这种速度需要的敏捷性和主动性在“物理”战争时代无异于天方夜谭，几乎是异想天开。空军研究实验室的卡莫尔·杰伯博士（Dr. Kamal Jabbour）指出：“网空敏捷性”不仅意味着迅速分析，而且还有对未来行为与效果的“预期”，以及对防御措施的有效实时安排。”[64] 这就要求情监侦部门在网空所有方面（速度、隐形、灵活性、适变性、以及使网空具有如此挑战性的其他各重大因素）都保持领先。[65] 正在进行的科技计划，比如《2025 年网空愿景》，提供了一个宝贵的起点，我们可以藉此了解这些问题并设计解决方案。空军部长迈克尔·唐利已经指挥空军领导班子积极部署，为实现此远景开拓道路。

自动化与可视化

网空数据如此浩瀚，恰如东方智语：“眩目之亮一如遮目之暗，均可致盲。”[66] 目前，网络传感器收集的数据量达到拍字节（petabytes），尧字节（yottabytes）的时代也为时不远。[67] 目前的数据收集量已经使我们无法招架，难以识别和淘出“真金”，也无从有效分析或处理成可操作的情报。因此，网空情监侦“要求我们开发算法语言和可视化能力，使网空活动智能化。”[68] 在这个等式的一边，我们需要取得能实现情监侦分析自动化的技术、操作图像和预测性软件，并为此得到人力和财力支持；在等式的另一边我们需要加上人才这个同样重要、甚至更重要的变量。

招聘与训练

我们中许多人都是所谓的数字时代移民。我们最初接触集成电路的亲身经历大概始于二十世纪七十年代的古董计算器、电子手表、也许还有早期的电子游戏机。网空的出现及其快速发展，一直令那些刚步下模拟技术之船——自愿或非自愿地——又步入数码新世界的人们感到苦恼、甚至畏惧。我们的下一代军人则属于另一种类。他们出生的

消息，可能是通过电子邮件公布于世；他们的生活中，大概从来不会经历没有电脑的时刻；他们全然不同于父辈的航空兵，但同样是世界上最优秀的军人。不过，对于玩了九年“使命召唤”电子战争游戏并主要由此获得战争概念的这一代人来说，美国空军的“飞行—战斗—必胜”座右铭自有其不同的含义，这一代人在数字化环境中长大，可能是整个网空领域最宝贵的资产。国家安全局局长兼美国网空司令部司令基斯·亚历山大上将（Gen Keith B. Alexander）显然认识到了这一点，他最近在一次自称为黑客大会的聚会上作了一次征兵宣传。[69] 需要的人才就在那里，而且人才济济。一旦被招入伍，这些人才只需接受网空作战的上层标准训练。但是这将要求“有扎实强大的技术及分析专业知识”——这些知识还必须不断更新才能适应网空领域的爆炸式进化。[70] 尽管詹姆斯中将声称：网空情监侦训练正在改善，但这项任务尚未完成。[71] 鉴于网空的不断进化，进一步完善空军技术专业编码体系、研究生课程、特定的适应性在职训练等，必须继续列为网空情监侦的首要优先任务之一。

网空情监侦的“正常化”

人力资源与训练、以及材料与技术，近来引起了国防部和空军的多项高级计划的关注，其中包括空军首席科学家的《2025 年网空愿景》研究、2012 年空军网空峰会、国防部的网空战略组合评估。具体成果——及其由此带来的未来网空情监侦能力——将取决于这些努力的结果、财政状况、持续演变的网空威胁与机遇等。然而，概念上讲，关于网空情监侦正常化的工作在今天就能、也应该开始。詹姆斯中将和其他空军情监侦领导人一直极力坚持认为：欲求情监侦有效运作，必须做到无缝衔接和抹除域间界线。情监侦在于为决策者投送及时、相关、可操作的情报，搜集情报信息的地点和方式对终极目标而言相对无关紧要。这样看来，正常化涉及到拆除我们在所有网空领域内外竖起的各自为阵的“烟囱”型指挥关系，承认对使命最重要的是从最终分析中获得的有用信息本身，而不是我们获取信息的方式或领域。鉴于网空领域的独特性、我们在该领域作战的相对生疏、作战计划有待实战验证等，我们在思维方式和体制上仍有许多障碍需要清除。然后，网空情监侦才能像天空情监侦和太空情监侦那样获得充分理解、承认和利用。说到底，这是一个教育和领导问题；但是在做好教育和领导之前，我们首先必须清楚认识到：网空本身已经形成一个领域，它像其它领域那样，以本质上相同的方式为情监侦带来了需求和机遇。在并不久远的过去，太空情报运作也曾有过生疏的、概念破碎的时期，但是它对作战效力的贡献却随着本身的成熟而迅速增长。

保护公民自由和隐私权

然而，对网空情监侦的各种人力物力投资，都必须坚守政府保护公民自由和宪法权利的义务。[72] 辛普森上校承认：“目前尚处婴儿期的网空法律和政策为情监侦运作造成权限与界限确定及管理方面的困难。”[73] 网空意识、安全和公民自由之间的平衡在不断演变，需要连续关注，并可对公众信任产生相当大的影响。[74] 对情监侦部门来说，这不只是一个次要的担忧。军人必须服务公民和捍卫宪法，因此在这些问题上应始终保持警觉和严格遵守规程。尽管今日网空法规仍模糊不清，也无论将来会出现什么相关的法院裁定，整个情报部队必须坚定不移地保护宪法及每个公民的隐私权。

结语

过去百年来，空军及其前身已经展现了征服新作战领域的强大能力——首先是天空，之后是太空。两次征服过程中，情监侦作战都证明对开创和维持新领域发挥了关键作用。相较而言，网空尽管有其种种独特属性，也同样拥有与前两个领域相同的根本特征：一旦缺少及时、相关、可操作的情监侦，其它所有军事活动的成功就只好听凭运气。这个新领域的将士们正遇到重重困难，但将作战成败付诸运气不是我们的选择。[75] 网空情监侦面临的困难有时似乎无法解决，但是我们不可迷惑于表象。当年空中力量也曾风驰电掣般快速发展和成熟，造成巨大的思维错位和滞后；在此之后开发浩瀚太空的几十年里，同样的现象再次发生。毫无疑问，现今我们又进入一个新的作战领域，必定遭遇许多同样的智力成长之痛。然而我们应该坚信：只要坚持不懈地深入全面了解网空，定能克服这些烦恼，网空情监侦帮助我们了解网空，又反过来加快网空情监侦的发展。为了继续这种积极的趋势，我们必须投资；要投资，我们就必须获得政府领导的承诺；但是要承诺，我们首先必须充分了解我们作为一支空军和一个国家所面临的挑战和机会以及其之性质和程度。情监侦作战是获得这种了解的关键——人类过去征服其他各种领域如此，现在征服网空亦然。♣

注释:

1. 在《神经漫游者》(Neuromancer）这本书中，威廉·吉布森（William Gibson）预言性地杜撰了“网空”（Cyberspace）一词来假设一种科幻奇思：“数亿人每日体验共意幻觉……从人体系统的每个计算机库里提取数据，无法想象的复杂性。”参看 William Gibson, Neuromancer (New York: Ace Books, 1984), 第 69 页。

2. 联合作战准则把网空界定为“信息环境内的一个全球性领域，由相互依存的信息技术基础设施网所组成，包括因特网、电信网、计算机系统、嵌入式处理器和控制器。”参看 Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms [联合作战准则 JP 1-02：国防部军语辞典], 8 November 2010 (as amended through 15 August 2012), 77, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. 然而笔者同意 Daniel Wasserbly 所说：“‘网空’本身就是一个如此模糊的概念，仅仅为了确定它的基本原理以及它如何影响军事领域就已经花费了数年的计划时间和人力。”参看 Daniel Wasserbly,“Charting the Course through Virtual Enemy Territory”[制定突破敌方虚拟领土的方针], Jane's International Defence Review, 44, no. 5 (May 2011): 60。或者如美国空军退役将军 Michael V. Hayden 所观察：“很少有什么事比这个现象更模糊，更缺乏明确理解，但却如此被看重被热论。”参看 Michael V. Hayden,“The Future of Things 'Cyber' ”[未来‘网络’之事], Strategic Studies Quarterly, 5, no. 1 (Spring 2011), 3, http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf.

3. 本文不讨论威胁——有关这个主题的文字资料就像威胁本身那样包罗万象且五花八门。然而，在所有军事行动中，对威胁的有效响应始于概念健全、计划周密、执行得当的情监侦。

4. 关于 CYBINT（网空情报），参看 Dr. Kamal T. Jabbour, 50 Cyber Questions Every Airman Can Answer [每个航空兵都应能回答的 50 个网空问题], (Wright-Patterson AFB, OH: Air Force Research Laboratory, 7 May 2008), 20, http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf; 关于 CYBINT 与信号情报的关系，可参看 Air Force Doctrine Document (AFDD) 2-0, Global Integrated Intelligence, Surveillance, & Reconnaissance Operations [空军作战准则 AFDD 2-0：全球一体化情报 / 监视 / 侦察作战], 6 January 2012, 40, http://www.e-publishing.af.mil/shared/media/epubs/afdd2-0.pdf; 关于 Frederick J. Wettering 所描述的公开来源情报，参看“The Internet and the Spy Business”[互联网和间谍工作], International Journal of Intelligence and Counterintelligence, 14, no. 3 (Fall 2001), 344; 另参看“Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025”[2025 年网空远景：2012-2025 年美国空军网空科学技术愿景], draft, AF/ST TR 12-01, 1 September 2012, 42.

5. Ben Iannotta,“Voice for Balance”[呼吁平衡之声], DefenseNews, 1 November 2011, http://www.defensenews.com/article/20111101/C4 情监侦 01/111010318/Voice-balance.

6. 从写这篇文章开始时算，作者在过去的几个月里已多次亲身经历。

7. Larry D. James 中将 2012 年 7 月 30 日与笔者交谈。

8. Air Force Policy Directive 10-17, Cyberspace Operations, [空军政策指令 10-17：网空作战], 31 July 2012, 3, http://www.e-publishing.af.mil/shared/media/epubs/AFPD10-17.pdf.

9. Intelligence and National Security Alliance, Cyber Intelligence: Setting the Landscape for an Emerging Discipline [网空情报：设置新兴学科的景观], (Arlington, VA: Intelligence and National Security Alliance, September 2011), 14, https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/Sept_ISOAG_CyberIntel.pdf; 另参看 AFDD 3-12, Cyberspace Operations [网空作战], 15 July 2010, 24, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf, 它指出“运用全频谱网空效应需要一个多元信息分析途径”和“聚焦全源网空的情监侦。”

10. Robert P. Otto 少将 2012 年 8 月 14 日与笔者书面交谈。

11. 见注释 9 中 AFDD 3-12《网空作战》，第 49 页。

12. Clay Wilson, Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues [信息战、电子战和网空战：能力与相关政策问题], CRS Report for Congress, (Washington, DC: Congressional Research Service, 20 March 2007), 5, http://www.au.af.mil/au/awc/awcgate/crs/rl31787.pdf.

13. Bryan Krekel, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation [中华人民共和国进行网空战和计算机网络利用的能力], (McLean, VA: Northrop Grumman Corporation, 9 October 2009), 8-9, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

14. Dr. Kamal Jabbour,“The Science and Technology of Cyber Operations”[网空作战的科学技术], High Frontier, 5, no. 3 (May 2009): 11, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf; 另参看注释 4 中“2025 年网空远景”，第 20 页；另参看 Air Force Space Command, Functional Concept for Cyberspace Operations [网空作战的职能概念], (Peterson AFB, CO: Air Force Space Command, 14 June 2010), 7; 另参看 Lt Gen Michael J. Basla,“Cyberspace from a Service Component Perspective”[从军种视角看网空], (address, Cyberspace Symposium, US Strategic Command, 15 November 2011), http://www.afspc.af.mil/library /speeches/speech.asp?id=686. 在此讲话中，Basla 中将把网空态势感知描述为“对作战空间作战情况（包括联合作战网、空军网、友好或非友好部队部署等状况）的了解。”

15. The Manual for the Operation of the Joint Capabilities Integration and Development System [联合能力集成与开发系统操作手册], (Washington, DC: Joint Staff J8 / Joint Capabilities Division, Pentagon, 19 January 2012), https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=1517681, 此文件把联合能力领域“作战空间感知”界定为“通过利用情报、监视、侦察、气象、海洋等全源信息，来了解对国家和军事决策起影响作用的作战环境的部署、意图、特点及状况之能力”（B-B-2）。要说明态势感知的个人认知方面，最好的例子也许是 John Boyd 的 OODA（观察、定向、决定、行动）决策环理念，此理念后为单座战斗机飞行员广泛接受。可参看 Col Phillip S. Meilinger, ed., The Paths of Heaven: The Evolution of Airpower Theory [登天之道：空权演变理论], (Maxwell AFB, AL: Air University Press, 1997), xxiii; 另参看 Maj David S. Fadok,“John Boyd and John Warden: Air Power's Quest for Strategic Paralysis”[约翰・博伊德和约翰・沃登：空中力量追求战略性瘫痪打击], (Maxwell AFB, AL: School of Advanced Airpower Studies, 1995), 13.

16. Martin Libicki,“Cyberpower and Strategy”[网空力量与战略], (remarks at the 8th International Institute for Strategic Studies Global Strategic Review,“Global Security Governance and the EmergingDistribution of Power,” Sixth Plenary Session, 12 September 2010), [3], http://www.iiss.org/EasySiteWeb/getresource.axd?AssetID=46892&type=full&servicetype=Attachment.

17. Lt Col Steven E. Cahanin, USAF,“Principles of War for Cyberspace”[网空的战争原则], research report, (Maxwell AFB, AL: Air War College, Air University, 15 January 2011), 1, http://www.airpower.au.af.mil/digital/pdf/articles/Jan-Feb-2012/Research-Cahanin.pdf.

18. 见注释 2 中 Michael V. Hayden“未来‘网络’之事”，第 4 页。

19. 比如，把今日的网空与其二十世纪九十年代早期相比，我们也许看到某些相似之处，诸如电子邮件、留言板、网联、信息库等。但现在回想起来，一些根本性的变化，诸如无处不在的社交媒体、视频流、网上语音视频通信、移动连接，还有今日复杂精密又无孔不入的网络威胁等，都远远超越了甚至二十年前最大胆的预测。

20. 见注释 17 中 Cahanin“网空的战争原则”，第 2 页；另参看 Brookings Institution, Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch [网空的威慑：与 Ralph Langner 和 Dmitri Alperovitch 辩论

正确战略问题], (Washington, DC: Brookings Institution, 20 September 2011), 2, http://www.brookings.edu/~/media/events/2011/9/20%20cyberspace%20deterrence/20110920_cyber_defense.pdf; 另参看 Paul W. Phister Jr.,“Cyberspace: The Ultimate Complex Adaptive System”[网空：最终的综合自适应系统], International C2 Journal, 4, no. 2 (2010-11): 13-14.

21. 见注释 17 中 Cahanin“网空的战争原则”，第 2 页。

22. “Remarks of the Honorable Michael B. Donley, Secretary of the Air Force[空军部长唐利在空军协会网络未来研讨会上的讲话], Air Force Association Cyber Futures Conference, Gaylord National Resort, Friday, March 23, 2012, 3, http://www.af.mil/shared/media/document/AFD-120326-056.pdf.

23. Department of Defense, Department of Defense Strategy for Operating in Cyberspace [国防部对网空作战的战略], (Washington, DC: Department of Defense, July 2011), 2, http://www.defense.gov/news/d20110714cyber.pdf.

24. 见注释 17 中 Cahanin“网空的战争原则”，第 3-4 页。

25. Paul Cornish et al., On Cyber Warfare [论网空战], Chatham House Report (London: Chatham House [Royal Institute of International Affairs], November 2010, 29, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

26. 虽然太空无限大，或有限但在扩大或缩小（理论各不相同），但是人类的太空空间，也就是说人类已经建立了或多或少永久性存在（即便极遥远）的空间，几乎完全局限在我们自己的太阳系内。除了阿波罗月球登陆和行星际、月球、或太阳探测之外，人类所及空间位于距地球表面 50-22000 英里之间。

27. 见注释 20 中 Brookings Institution“太空的威慑”第 2 页。到 2012 年的年中，我们每一天的每一分钟都会看到网空中传输着：长达 48 小时的 Youtube 视频、204166667 封电子邮件、2000000 次 Google 搜索、684478 个 Facebook 帖子、571 个新因特网网站、27778 篇 Tumblr 博文、100000 多条 Twitter 信息。参看 Oliur Rahman,“How Much Data Is Created on the Internet Every Minute?”[因特网上每分钟产生多少数据 ?], Ultralinx, 24 June 2012, http://theultralinx.com/2012/06/data-created-internet-minute.html.

28. 参看注释 4 中“2025 年网空远景”，第 9 页。

29. Richard M. Crowell, War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare [信息时代的战争：二十一世纪战争中的网空作战入门], (Newport, RI: Naval War College, 2010), 21, http://www.carlisle.army.mil/DIME/documents/War%20in%20the%20Information%20Age%20-%20A%20Primer%20for%20Cyberspace%20Operations%20in%2021st%20Century%20Warfare%20-%20R%20M%20%20Crowell.pdf.

30. 与大众所信相反，网空的活动不是以光速发生，确切地说，网空操作以电子速度进行。光的传播速度大约每秒 186000 英里，而电子——由于有质量——的传播速度“只是”光速的 2/3，即每秒约 125000 英里。参看注释 4 中 Jabbour“50 个网空问题”，第 11 页。

31. Mike McConnell,“Cyber Insecurities: The 21st Century Threatscape”[网空的不安全：二十一世纪威胁景观], 收录于 America's Cyber Future: Security and Prosperity in the Information Age [美国的网空前景:信息时代的安全与繁荣], vol. 2, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for a New American Security, June 2011), 25-39, http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf.

32. Robin Geiβ,“The Conduct of Hostilities in and via Cyberspace”[网空中的敌对行为], Proceedings of the Annual Meeting, (American Society of International Law) 104 (24-27 March 2010): 371; 另参看注释 21 中 Crowell“信息时代的战争”，第 21 页。

33. 严格地讲，即使世界大战的情况也不是如此，因为盟军指挥官不必担心轴心国有可能从瑞士或斯威士兰突袭。

34. 见注释 32 中 Geiβ“敌对行为”，第 371 页；另见注释 17 中 Cahanin“网空的战争原则”，第 5 页。

35. Susan Freiwald,“Electronic Surveillance at the Virtual Border”[虚拟边界的电子监视], Mississippi Law Journal, 78, no. 2 (Winter 2008): 329, http://www.olemiss.edu/depts/ncjrl/pdf/ljournal09Freiwald.pdf; 另见注释 32 中 Geiβ“敌对行为”，第 371 页；另见注释 17 中 Cahanin“网空的战争原则”，第 5 页。

36. 见注释 20 中 Brookings Institution“网空的威慑”，第 15 页;另见注释 29 中 Crowell“信息时代的战争”，第 21 页。

37. 例如：网空“基地”、网空“空域”或网空“兵力结构”。

38. 见注释 31 中 McConnell“网空的不安全”,第 61 页;另参看 Gregory C. Radabaugh,“The Evolving Cyberspace Threat”[进化中的网空威胁], (working paper, Air Force Intelligence, Surveillance, and Reconnaissance Agency, August 2012), 8; 另见注释 25 中 Cornish et al“论网空战”，第 30 页；另见注释 29 中 Crowell“信息时代的战争”，第 21 页。

39. 见注释 9 中 Intelligence and National Security Alliance“网空情报”，第 7 页。关于类似的评估，另参看 Kevin Coleman and John Reed,“Cyber Intelligence”[网空情报], DefenseTech.org, 3 January 2011, http://defensetech.org/2011/01/03/cyber-intelligence/.

40. 见注释 17 中 Cahanin“网空的战争原则”，第 5 页。

41. House, House Armed Services Subcommittee, Cyberspace Operations Testimony [Keith Alexander 上将在众议院武装部队小组委员会上就网空作战作证], Sept. 23, 2010, [1], 111th Cong., 2nd sess., http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf. 当时的众议院武装部队委员会主席 Ike Skelton 议员在开幕致词中如此说。

42. Kenneth Geers, Sun Tzu and Cyber War [孙子与网络战], (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 9 February 2011), [4], http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf. 关于溯源之挑战的更透彻的讨论，参看 Martin C. Libicki, Cyberdeterrence and Cyberwar [网空威慑和网空战争], (Santa Monica, CA: RAND Corporation, 2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

43. 见注释 14 中 Air Force Space Command“网空作战的功能概念”，第 10 页。

44. Rand Waltzman,“Anomaly Detection at Multiple Scales”[多规模异态检测], (presentation, DARPA Cyber Colloquium, Arlington, VA, 7 November 2011), slides 3-4.

45.“洋葱路由”指的是一项技术，最初由海军发明，目的是在网上传送邮包过程中隐蔽其出处和内容。邮包的传送是通过一个随机挑选的代理服务器网，同时依次经过不同级别的加密和随后的解密，然后作为普通文本被送达目的地。W. Earl Boebert,“A Survey of Challenges in Attribution”[对溯源挑战的调查], 收录于 National Research Council of the National Academies, Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy [“慑阻网空攻击：为美国国家战略和政策建言”研讨会论文集], (Washington, DC: National Academies Press, 2010), 43-46.

46. 见注释 3 中 Jabbour“50 个网空问题”，第 9 页。

47. 第 659 情监侦大队指挥官 Daniel Simpson 上校 2012 年 8 月 8 日与笔者交谈。第 659 大队是美国空军主要的网空情监侦部队，承担“数字网络利用分析和数字网空情报工作”。参看 Capt Karoline Scott,“New 情监侦 Group Supports Cyber Operations”[新建情监侦大队支援网空作战], Air Force News Service, 10 September 2010, http://www.af.mil/news/story.asp?id=123221324; 另参看注释 9 中 AFDD 3-12《网空作战》，第 24 页。

48. Kristin Quinn, Vago Muradian, and Marcus Weisgerber,“The Pentagon's New Cyber Strategy”[五角大楼的新网空战略], DefenseNews, 18 August 2011, http://www.defensenews.com/apps/pbcs.dll/article?AID=2011108180316.

49. 见注释 42 中 Libicki“网空威慑和网空战争”，第 96 页。

50. 见注释 2 中 Wasserbly“制定方针”，第 60 页。

51. Decian McCullagh,“House Passes CISPA Internet Surveillance Bill”[众议院通过 CISPA 因特网监视议案], ZDNet, 27 April 2012, http://www.zdnet.com/news/house-passes-cispa-internet-surveillance-bill/6360341. 民主党国会议员 Jared Polis 表示反对,声称 CISPA(计算机情报共享和保护法案)将“以网络安全的名义,放弃执行有史以来制定的每一条隐私法……允许军队和国家安全局违背我们建国所依据的每一条原则，在美国的土地上暗中监视美国人。”另参看 Sanjay Goel,“Cyberwarfare: Connecting the Dots in Cyber Intelligence”[网络战：连接网空情报中的各分散点], Communications of the ACM , 54, no. 8 (August 2011): 137; 另参看 Mike McConnell,“Mike McConnell on How to Win the Cyber-War We're Losing”[如何打赢我们正在输掉的网空战], Washington Post, 28 February 2010, B01, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. 除了像“美国公民自由同盟”这种普通维权组织外，拥护隐私权组织还包括“电子边疆基金会”(它在网站 https://ssd/eff/org 中提供正当防卫监视的辅导课程)、savetheinternet.com（主要鼓吹“因特网自由”)、电子隐私信息中心、民主与技术中心、技术解放阵线、OpenNet（该组织在网站 http://opennet.net/about-oni 宣称“我们的使命是调查、揭露和分析因特网过滤和监视做法”)。根据笔者的意见和经验，自从 1976 年的教会委员会报告以来，没有哪一类情报界的活动在美国招致了如此热切的关注和强烈的公众反弹。

52. 要深入了解最近关于网空隐私、搜查和查封及其他宪法规范的法律辩论，可参看 Susan W. Brenner,“Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force”[第四修正案的未来：远程计算机搜索和虚拟部队的使用], Mississippi Law Journal, 81, no. 5 (2012): 1229-62; 另参看 Timothy Casey,“Electronic Surveillance and

the Right to Be Secure”[电子监视和安全保障权], University of California-Davis Law Review, 41, no. 3 (February 2008): 977-1033; 另参看 Elizabeth Gillingham Daly,“Beyond 'Persons, Houses, Papers, and Effects': Rewriting the Fourth Amendment for National Security Surveillance”[超越“人身、住宅、文件和财产”：重写为国家安全监视第四修正案], Lewis & Clark Law Review, 10, no. 3 (Fall 2006): 641-71; 另参看 Dan Fenske,“All Enemies, Foreign and Domestic: Erasing the Distinction between Foreign and Domestic Intelligence Gathering under the Fourth Amendment”[所有外国和本国的敌人：第四修正案消除外国和本国情报搜集的区别], Northwestern University Law Review, 102, no. 1 (2005): 343-81; 另参看注释 35 中 Freiwald,“Electronic Surveillance”[电子监视], 329-62; 另参看 John N. Greer,“Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and Protection of Privacy Rights and Civil Liberties in Cyberspace”[网空方枘难容法律圆凿：美国国家安全局、合法性、网空的隐私权及公民自由保护], Journal of National Security Law and Policy, 4, no. 1 (2010): 139-54; 另参看 Orin S. Kerr,“Applying the Fourth Amendment to the Internet: A General Approach”[把第四修正案用于因特网：通用做法], Stanford Law Review, 62, no. 4 (April 2010), 1005-49; 另参看 Mike McNerney,“Warshak: A Test Case for the Intersection of Law Enforcement and Cyber Security”[Warshak：执法和网络安全交会的一个验证案例], University of Illinois Journal of Law, Technology and Policy 2010, no. 2 (Fall 2010), 345-57; 另参看 Amanda Yellon,“The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications”[第四修正案的新边疆：把第四修正案用于电子通信的司法理念], Journal of Business & Technology Law, 4, no. 2 (2009): 411-37; 另参看 Mark D. Young,“Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security”[现代技术时代的电子监视和对国家安全形成的威胁], Stanford Law & Policy Review, 22, no. 1 (2011), 11-39. 这些论著及所述案例提出了一些有代表性的问题，归纳如下：

- 是否可把计算机比作“容器”受《第四修正案》保护而免受“不合理搜查和查封”？
- 是否应将网上通信与封口信件同等对待受隐私权和宪法权利保护（内容与非内容对比）？
- 对具体个人网络通信（尤其是期望受到隐私保护的电子邮件和文本）的监视是否也要接受像对窃听一样的限制和制约？
- 网空情报专业人士如何保证遵守 12333 号行政命令《美国情报活动》,从而限制为抵御外国威胁的情报搜集（亦即如何知道受监视或搜集情报的对象是不是受宪法与行政保护的“美国人”）？
- 总的问题是，个人权利与政府责任如何平衡才能保障双方都不遭受国内外的威胁？

53. 见注释 52 中 McNerney“Warshak：执法和网络安全交会的一个验证案例”，第 346 页。

54. 见注释 14 中 Air Force Space Command“网空作战的功能概念”，第 15 页。

55. 见注释 42 中 Libicki“网空威慑和网空战争”，第 155-156 页。

56. 见注释 17 中 James 中将与笔者交谈。

57. RADM J. Michael McConnell 于 2012 年 8 月 23 日与笔者电话交谈。

58. 参看 William J. Lynn III,“Defending a New Domain: The Pentagon's Cyberstrategy”[捍卫一个新领域：五角大楼的网空战略], Foreign Affairs, 89, no. 5 (September-October 2010): 99.

59. Ned Moran,“A Cyber Early Warning Model”[一个网空早期预警模型], 收录于 Jeffrey Carr, Inside Cyber Warfare [网空战内幕], (Sebastopol, CA: O'Reilly Media, 2010), 200; 另参看注释 42 中 Geers“孙子和网络战”，第 10 页。

60. Gregory C. Radabaugh,“The Evolving Cyberspace Threat”[进化中的网空威胁], (working paper, Air Force Intelligence, Surveillance, and Reconnaissance Agency, August 2012), 9.

61. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin,“Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”[根据对敌方战役和入侵杀伤链的分析而开展的由情报驱动的计算机网络防御], (paper presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, 17-18 March 2011), 3, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf; 另参看注释 59 中 Moran“网空早期预警模型”,第 208 页；另参看注释 60 中 Radabaugh“进化中的网络威胁”，第 9 页。

62. 见注释 61 中 Hutchins“由情报驱动的计算机网络防御”，第 3 页。

63. 见注释 57 中 McConnell 与笔者电话交谈。

64. Dr. Kamal Jabbour,“Cyber Vision and Cyber Force Development”[网空远景与网空部队发展], Strategic Studies Quarterly, (Spring 2010), 65, http://www.au.af.mil/au/ssq/2010/spring/spring10.pdf.

65. 难怪空军中有些网络战士戏称自己为“日本武士”。

66. Richard Stiennon, Surviving Cyberwar [打赢网络战], (Lanham, MD: Government Institutes, 2010), 121.

67. 一个拍字节（petabyte）等于 10 亿个吉字节（gigabyte）；一个尧字节（yottabyte）等于 10 亿个拍字节。

68. 见注释 3 中“2025 年网空远景”，第 40 页。

69. Damon Poeter,“DefCon: NSA Boss Asks Hackers to Join the Dark Side”[国防战备：美国国家安全局老板邀请黑客加入黑边行列], PC Magazine, 29 July 2012, http://www.pcmag.com/article2/0,2817,2407783,00.asp.

70. 见注释 9 中 Intelligence and National Security Alliance“网空情报”，第 14 页。另参看 Wayne Michael Hall and Gary Citrenbaum, Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments [情报搜集：如何在复杂环境中规划和执行情报搜集], (Santa Barbara, CA: Praeger, 2012).

71. 见注释 17 中 James 中将与笔者交谈。另参看注释 47 中 Simpson 与笔者交谈，Simpson 表示：“训练是另一个需要克服的挑战，”因为“目前缺少进行细致网络空分析的技术能力。”

72. 见注释 58 中 Lynn“捍卫一个新领域”，第 103 页。

73. 见注释 47 中 Simpson 与笔者交谈。

74. 比如，2010 年的一项调查发现，88% 的美国人相信他们在网上应该享有与物理领域里一样的合法隐私权保护；只有 4% 的人持不同意见。参看 US Department of Commerce, Comments of Digital Due Process, in the Matter of Information Privacy and Innovation in the Internet Economy [就因特网经济中信息隐私和创新的问题，对数码化合法诉讼程序的评论], docket no. 1004020174-0175-01 (Washington, DC: US Department of Commerce, National Telecommunications and Information Administration, 14 June 2010), 4, http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf.

75. 见注释 58 中 Lynn“捍卫一个新领域”，第 99 页。

马修·M·赫尔利，美国空军上校（Col Matthew M. Hurley, USAF），美国空军军官学院毕业，华盛顿大学文科硕士，空军大学军事艺术科学硕士，俄亥俄州立大学博士，现任华盛顿特区五角大楼美国空军总部情监侦副参谋长办公室准则与政策整合主任，在此职位上他确保空军情监侦规则和最佳做法被适当纳入联盟、联合及空军作战准则与政策文件中。赫尔利上校是职业情报官，曾服务于支持空中机动司令部、驻韩美军、驻欧美国空军及中北欧联盟空军的岗位，包括派赴西南亚和非洲之角的应急部署。他曾获得 Ira C. Eaker 奖，并于 1989 年获空军历史基金会颁发的空军重大历史研究奖。他的最新著作《飞行中：以色列空中力量对阿克萨群众起义，2000-2005 年》，由阿拉巴马州马克斯韦尔空军基地的空军研究所于 2010 年出版。