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。

网空中的联合目标选定

Joint Targeting in Cyberspace

史蒂文·J·斯马特，美国空军少校（Maj Steven J. Smart, USAF）

美国每天都依赖我们的数字基础设施，因此保护这项战略资产是国家安全的一项优先。

—— 奥巴马总统，2010 年

网空安全很明确是国家安全的一项优先，但是美国武装力量在这个新领域的作用并不明确。美军于 2010 年设立网空司令部之后，网空军事化和网空“战争”如何进行便成为政府决策者之间一个中心争议话题。[1] 更复杂的是，至今无法确定如何应用国内法律和政策指导方针以及针对武力战争的国际条约来管辖网空行为。[2] 尽管存在这种不确定性，国防部的政策要求其下属单位“在所有的武装冲突（无论其性质如何）以及在所有的其他军事行动中遵守战争法。”[3] 目前尚不清楚华盛顿的决策者们会给军方界定网空领域的什么作用和责任，但是国防部应该为在网空执行军事行动做好准备。为了有效地执行这一使命，国防部应将经过时间考验的联合目标选定原则在略加修改之后应用到网空作战。[4] 本文探索国防部联合作战准则 JP 3-60《联合目标选定》（Joint Targeting）应用于网空军事行动的可行性，并对网空联合目标选定提出一些建议。[5]

联合目标选定的基本原则

在论述 JP 3-60 是否适用于网空目标选定之前，我们必须了解这部文件的基本原则、应用的理由，以及作战准则与法律之间的关系。“联合作战准则是指导美国武装力量之运用的基本原则，”并且“各级［指挥官必须］确保其部队的作战行动遵循‘战争法’”，因为“战争法对美国有约束力。”[6] 联合作战准则体现了美国对遵守国际法的承诺和最佳作战实践。“战争法”包含协定国际法（各国之间的条约和协议）和惯例国际法（基于各国的习惯做法）。[7] 惯例国际法来自各国的习惯做法，即各种法规条令（包括公布的作战准则）所反映的官方政府行为。因此，联合作战准则不仅加强有约束力的法律义务，而且推动惯例国际法的发展。

简而言之，构成现代战争法基础的主要信念可分为两大部分，一是战争的作战规则，二是对冲突各方及其旁观者的对待方式：《海牙公约》和《日内瓦公约》分别涵盖这两个部分。[8] 此外，《联合国宪章》载有联合国成员国对其他国家“使用武力”时应遵循的义务。[9] 国内法（联邦法律和司法裁决）、美国政府政策、联合作战准则和军种作战准则以及交战规则具体规定美国武装力量应如何遵循这些国际义务。我们必须了解，无论是常规的还是具有任务针对性的军事作战准则或交战规则，都不可替代或取代战争法，而应该体现美国在具体形势下对相关国际原则的认同和履行。

我们可以将众多的规则、条例和准则归纳为五条适用于任何特定作战行动的简单原则。第一，使用武力的假设前提是存在采取军事行动的必要性（军事上有需要使用武力的合理理由以便执行任务）。[10] 第二，使用武力不得给平民或敌方部队造成不必要的痛苦。[11] 指挥官不仅必须将这条原则应用于潜

在的“附带损伤”（伴随的平民生命损失或平民财产毁损），而且必须将它应用于预定攻击目标——这条原则后来成为某些武器和弹药（例如：化学武器）禁用公约的基础。第三，使用武力必须区分或区别战斗人员和非战斗人员，而且不得故意攻击并未直接参与敌对行动的平民。[12] 简言之，作战人员必须使用具瞄准功能的武器，而且必须区分平民和敌方战斗人员——这是分析联合目标选定的基本指导原则，下文将详细论述。第四，军事行动强度必须成比例，换言之，它必须避免滥用武力而导致与预期军事优势不相称的过度附带损伤。[13] 第五，武装冲突各方必须展现专业军人品质，即保持“一定程度的公平……和相互尊重及信任。”[14] 这些原则既适用于规范一般的武力运用，更适用于指导具体的目标选定。

在军事界，目标选定往往是指双方军队交战或准备交战的一项行动。联合作战准则对目标选定的正式定义是：“根据作战要求和作战能力选择和排定目标、并确定适当打击手段的过程。”[15] 这个定义，尤其是目标的选择和手段的确定，最直接地要求遵循战争法的义务。战争法中的“区分原则”首先就是针对目标的选择而成立。军事目标是合法的目标，但是军队不可故意攻击平民，还应尽一切力量避免误伤无辜。[16] 因此，战争法规定军事指挥官和作战人员有责任尽可能准确地判别预期军事行动准备打击的目标，根据其性质和功能，确定是否归于打击范围。

军事作战准则进一步设定原则，引导军队履行其“区分”义务。联合作战准则文件 JP 3-60 就联盟或联合作战给出了有关目标选定的总体原则。军种作战准则文件，例如空军作战准则文件 AFDD 2-1.9《目标选定》，对联合作战准则进行补充，设定了具体适用于本军种主要责任的原则。[17] 这些原则归纳自最佳作战实践，吸取了美军和盟军在过去历次战役和作战行动中的集体经验。然而对于网空领域，至今没有任何军种被指定为主要责任者，至今也未在这个领域中积累出作战方面的最佳实践，因此只能套用其他作战领域的现有作战准则，作为网空作战策划和网空作战目标选定的依据。[18] 于是，JP 3-60 就顺理成章成为网空联合作战中指导目标选定的基本文件。

将现有作战准则用于网空领域

将现有军事作战准则（尤其是目标选定和战争法原则）应用到网空作战，在理论上讲很容易，但在实践中也许极为困难。网空战争同传统的武装冲突有本质差别。网空作战不同于过去的作战样式，敌方（包括敌对国家、犯罪组织、恐怖分子和黑客）能够从地球上任何地点发动网空攻击，速度快，成本低，可匿名，而且损害极大。现有的军事作战准则是基于国家之间的武力战争经验和理论，其战场几乎总是存在于物理可辨识和可理解的区域（天空、陆地、海洋和太空）。相比之下，网空战争发生在“同时存在于虚拟层面和物理层面的区域，贯穿于电磁频谱中的各种活动，电磁频谱则无缝穿越其他所有领域，跨越地理及经认同的政治界线。”[19]

网空战争和传统的武力战争有多大不同，它能在多大程度上反映现代军事模式的转变，自是仁者见仁智者见智，最好留待历史学家来研究。但是，物理世界与网空领域之间，就武装冲突及其参与者和手段 / 方法等而言，显然存在差异。差异则意味着挑战，当我们将现有法律、政策和军事作战准则应用于以键盘和鼠标为武器的作战样式时，就能意识到有多困难。

首先，网空战争的参与者并不限于国家指派的人员。网空攻击不同于传统的军事攻击，它不需要政府赞助。[20] 第二，攻击者不需要拥有昂贵的传统武器系统，只需要一台计算机、一个互联网连接和一些基本的网空知识。[21] 第三，在武力战场识别攻击来源比较容易，而要找到网空攻击的来源，则非常困难。例如，要找到发起某次导弹攻击的国家比较容易，因为导弹尺寸、速度、射程和弹头类型等关键“指纹”会指向拥有发起这次攻击的技术、意愿和知识的某几个国家。但是，网空攻击可从任何地方发起，而且攻击者可以是任何人，包括国家赞助的“黑客活动家”、非国家行为者，或者“挟着一部电脑随时发起攻击的政治狂热独行侠”。[22]

从网空战争与其难兄武力战争之间的关键差异，引出几个相关的问题。第一，能否指望甚至是国家指使的网空斗士在这个新领域中遵守基于传统武力战争概念的法律原则和军事作战准则？第二，我们是否需要为解决这些差异而制定专用于网空作战目标选定的新联合作战准则？

尽管作战领域不同，网空作战人员基本上和陆地、海洋和天空作战人员是一样的。这两类作战人员都依赖其对作战领域、作战环境和武器系统能力的了解。作战是一个极其复杂的过程，不可能将其简缩成指挥官可以勾选的一份程式清单。明智的指挥官或许能在具体的战役或战略环境中保持清醒，运用久经考验的战争真理，包括战争法的应用框架。网空战士只要对基于传统武力战争的法律原则和军事作战准则稍加修改，即可应用于网空作战，仍能取得预期的效果。同理，JP 3-60 如能依据网空特点稍加调整，就可继续作为指导美军在动能和非动能打击目标选定方面的基本准则文件。

网空的军事作战准则

直至不久前，只有一份联合作战准则文件专题论述网空领域的军事作战行动。[23] JP 3-13《信息作战》将信息作战（IO）定义为“电子战、计算机网络作战、心理作战、军事欺骗和作战行动安全保障的综合运用，与其它指定的支援能力和相关作战能力协同，以期影响、干扰、破坏或剥夺敌方的人工或自动决策机能，同时保护己方的决策机能。”[24] 就作战准则而言，由计算机网络攻击（CNA）和计算机网络防卫（CND）构成的计算机网络作战只是一个子集，和其他不同的行动类型一道组成一个更大的类别。作战准则确定上述各项作战能力是总体信息作战的核心，认为它们可帮助联合部队指挥官对敌方施加影响。但是，将它们集成为信息作战，则说明信息作战本身是一种特殊的作战样式，能快速整合入联合特遣部队。遗憾的是，各军种在进行人员训练时并未按照这个思路。它们目前只训练作战人员掌握一种或两种作战能力，例如电子战或心理作战。在计算机网络作战领域，很少有作战人员同时掌握 CNA 和 CND 能力。因此，信息作战分队在联合特遣部队充其量也只是一个“杰出的立柱体”（就是说，这些作战人员在其狭窄的领域内很内行，但对其他作战能力不甚了解）。在目标选定概念方面，这个问题尤其明显，JP 3-13 对这个主题没有提供指导。

既然认为这些作战能力是“核心”，JP 3-13 为什么对目标选定没有任何论述呢？我们可以想出三条理由。第一，目标选定是作战行动的关键部分，因此几乎每个军人对这个概念都有大致的了解，不必赘述。实际上，能成功地达成军事和政治目的的目标选定是一个非常复杂的过程，只有极少数人掌握这个能力。简言之，多数军事专业人员知道目

标选定的含义,但只有少数人知道如何去做。第二，JP 3-13 并未具体论述这些核心作战能力。它要求信息作战策划人员去参看其他一些作战准则的指导，其言外之意是，这些作战能力之间不一定像 JP 3-13 所断言的那样具有紧密关联性。在传统型军事行动策划者的头脑中，这些作战能力只是若干独特的、非常规的军事活动,很难纳入到作战计划中。第三，许多作战策划者认为“目标选定就是选定目标”，无论其平台或领域是什么，不必想得太复杂。

大多数网空作战策划者会声称他们了解军方准则所正式定义的和 JP 3-60 文件所论述的目标选定的一般概念。但是，他们将这个概念和定义应用到信息作战的各种核心作战能力时，实际情况可能大不一样。例如，一项策划中的心理作战行动也许会将一群外国听众作为“目标”，试图影响他们的行为和行动，但是一项电子战行动也许会将一个电台发射塔发出的信号作为目标。JP 3-13 认为信息作战的上述五种功能在作战行动中是相互关联的，但是该文件没有具体论述应该如何使用这些功能去选定敌方目标。[25] 于是，信息作战策划者和作战人员必须到有特定主题针对性的作战准则文件里去寻找指导。[26] 由于 JP 3-13 是唯一提供网络联合作战指南的准则文件，致使计算机网络作战策划者面临的问题更加复杂。[27] 因此，联合部队中的计算机网络作战策划者必须经常回过头去参看军种作战准则，在那里寻找指导。

最近，空军发布了作战准则 AFDD 3-12《网空作战》，对网空作战和信息作战加以区分。[28] 该文件是空军为理解、组织、训练和引导空军官兵进行网空作战而做出的最大努力。AFDD 3-12 在论述上简繁得体，对网空新手和专家均可适用，向空军官兵提供技术上可靠和作战中实用的引导，填补了联合作战层面缺乏网空作战指导文件的空白，因而值得称赞。更令人称道的是，该文件将联合作战原则与网空作战关联，向各类军事作战行动提供建议，并列出空军网空作战人员应遵循的基本原则。[29] AFDD 3-12 也许是国防部系统内论述网空作战最详尽的文件，如果将这样一份具有相当广度和深度的作战准则改写为联合作战准则，将让整个联合作战部队受益。不过，尽管 AFDD 3-12 论述了许多对于网空目标选定有用的问题，例如网空基础设施中的技术关系、信息保证、压缩决策周期、确定匿名者和攻击来源面对的挑战等，但它并没有具体论述网空目标选定本身。[30] 实际上，该文件要求读者参看 JP 3-60，表示该联合作战准则文件所列的原则、指导和理论适用于空军的网空作战。

一方面，现有的关于网空的国防部文件、联合作战准则或军种作战准则很少触及有关目标选定的主题，其原因也许是军方刚开始正式组建网空部队，或者是因为各军种没有积累很多的网空目标选定经验可供借鉴。[31] 另一方面，国防部领导人也许单纯地相信 JP 3-60 的目标选定原则很完善，可以方便地套用到网空领域的军事作战。无论原因为何，JP 3-60 即使没有直接提及网空领域，却仍是关于网空目标选定的重要的联合作战准则文件。

点评联合作战准则 JP 3-60

JP 3-60 分为三大部分：目标选定的基本原理、联合作战目标的选定程序，以及职责和责任。文件合乎逻辑地从目标定义开始，然后顺序论述目标确认、目标交战和损伤评估，最后讨论指挥责任和监督。这部文件简洁明了，执行目标选定的新手能够很快掌握

其基本原理。例如,文件用一份简单的图表(图 II-1：联合目标选定程序）阐明了作战目标选定的要素。[32] 理解了这个程序，就理解了目标选定。

联合目标选定程序快速列明对敌交战的对象、内容、地点、时间、原因和方式。[33] 在联合部队指挥官宣布期望的终局结果和目的之后，作战策划者便开始选择目标和排列打击顺序，以期实现指挥官期待的结果。目标选定后，下一步就是选择武器 / 能力匹配，做到既能确保交战成功又能尽量减少附带损伤。选定了具体武器，即决定了兵力分配，为任务策划提供了依据并促成其执行。任务完成后需要开展评估，按照预定指标衡量打击行动和效果，提交指挥官确定是否达到其目的或是否需要补选打击目标。对这整套程序，省略任何步骤都可能减弱打击效果；增加步骤则属多此一举。从法律角度看，指挥官若能遵守联合目标选定程序和作战准则所列的其他基本原则，辅之以指挥官的明智判断，应可确保作战过程符合战争法。

由此来看，JP 3-60 似乎是一部“即插即用”的指南，适合任何领域的目标选定。遗憾的是，有些分析家认为网空领域基本上具有和天空、陆地、海洋和太空一样的领域特性，而没有看到网空的独特性。

网空像其他领域一样，占据一个区域，是各国政府和企业界探索利用的对象，也是公司企业、国家和个人开展商务的媒介。对这个独特的媒介，“世人应学习欣赏其独有的优势；它是一个人造的架构。”[34] 计算机能几乎实时启动某个行动，也能几乎完全藏匿发动者和使用者。同样的网空基础设施，既为犯罪分子、恐怖团伙和敌对国家行使战争行动所用，也为工商企业及个人从事商业活动所用，这种共用性给网空军事作战行动蒙上一层“社会色彩”。[35] 在天空、太空和海洋领域，能够有效地威胁或挑战美国及其武装力量的敌方是极少数。相较而言，网空领域挤满了各色人等，不断有人对美国及其盟国，以及互相之间，进行施压、顶撞或恫吓。在这片如此混乱拥挤的战场中，用 JP 3-60 指导目标选定时势必在以下五个重要方面面临困难：(1) 确凿识别目标；(2) 判定目标位置；(3) 确定攻击来源；(4) 匹配作战能力 / 目标；(5) 评估潜在附带损伤。

首先，全球网空基础设施是军民并用，错综复杂，增加了确凿识别潜在网空目标的难度。JP 3-60 有两个章节论述目标识别：第 2 章“联合目标选定程序”和附录 E“目标选定的法律考量”。这两个章节都明确地指出，有效的和合法的军事目标需要具备某种程度的明确标识和特征，其识别和鉴定应在正常的或时间紧迫的目标选定程序中进行。这两个章节都没有讨论网空目标的瞬间即逝特点或独特性，也没有提到该独特性几乎只存在于军民共用媒介中。

作为示例，让我们假设作战策划者向联合目标选定协调小组提出三个目标，该协调小组的作用是“协助和协调联合作战部队的目标选定活动……确保符合［联合作战部队指挥官］任务优先顺序的要求。”[36] 提出的第一个目标是一辆坦克，第二个目标是一个网站，第三个目标是一个在线“角色”。最初，协调小组也许会确认那辆坦克是军事目标，但是认为那个网站和那个在线角色不是 JP 3-60 或战争法所定义的合格军事目标，因为这两者都不是物理意义上的物体，只是一种“1”和“0”构成的二进制公式组成。 这不是正确的评估。实际上，JP 3-60 并未把目标限定在实物世界，而是将目标定义为“可视

为交战或作战行动对象的某个**存在体**（entity）或物体（object）。作为被关注的可能的行动对象，它可以是一个区域、建筑群、设施、军队、设备、能力、功能、个人、群体、系统、**存在体**，或者一种行为”（粗体强调为笔者后加）。[37] 这个广阔的定义已经将那个网站和那个在线角色纳入其中。

与敌方坦克交战的合法性不言而喻，因为那件武器的唯一用途就是在武装冲突中实施毁杀；但是对网站和在线角色的战争法分析必须再进一步。对网站和在线角色都必须用“使用”,而不是“用途”,作为标准来判断。换言之，在发起策划的攻击时，敌方是否正在使用网站或在线角色来增强其作战能力或战争持续能力？如果是，则它们可能是合法的军事打击目标。不过我们很难确定这些双重用途物体、存在体或行为在网空中或通过网空对敌方作战过程实际做出贡献的确切时间，故而增加了交战难度。网空目标验证程序不同于武力战争目标验证程序，它要求持续更新验证情报，并以近实时状态进行确凿识别。

第二，网空中的目标位置判定具有独特的挑战性。JP 3-60 和战争法论述了对主权国家有实体侵犯情形下的目标定位。作战准则和法律都没有考虑到某个目标同时存在于地球上几个不同地点的情形，或是在多个冲突区域产生效应的情形，而此等情形却可能在网空发生。例如，敌方可以通过同时寄存于几个不同国家的服务器，在其中建立若干网站，实施指挥和控制功能，并且可以频繁地移动这些网站，以挫败任何打击。于是，问题出现了：适用于军事行动策划者和作战人员的特定交战规则也许禁止在联合作战区域以外的某些地方采取作战行动，即使敌方使用不断变换的全球网络从那些地方发起攻击。这个困境引发意义重大的争论。目标是什么？是在联合作战区域内实体存在的敌方，还是散布在全球的敌方指挥控制网络？如果由于地理位置的原因而无法进行交战，军事行动策划者自然需要重新选定确切的目标。那么，这个目标究竟是部署在战场上的部队还是他们的网络？

第三，把网空中的作战能力、设备及其使用究源于某个特定的、公开宣战的敌方，是非常困难的。尽管这种追究可以视为“确凿识别目标”阶段的一部分，本文却将之单独列出，以便说明进攻性网空目标选定和防卫性网空目标选定的区别。[38] 人在网空可匿名存在，这种特征使敌方能掩其行踪，却导致将非战斗人员或其他存在体当作替罪羊。敌方可以劫持无辜平民、群体或政府的计算机,将它们用作“僵尸网络”,发起网空攻击。当受攻击方进行初步罪证调查时，可能会将攻击源指向无辜的非战斗人员，而不是真正的攻击者。严格地说（取决于损害程度），战争法可以将此等攻击视为背信弃义的战争罪。从现实角度说,如果攻击持续不断(例如:分布式拒绝服务)，受攻击方是否必须确凿识别每个目标、并且基本上能将攻击来源追溯到某个已公开宣战的敌方,才可以针对“攻击”计算机采取防卫措施？值得庆幸的是，如上所述，战争法承认内在的自卫权（注重威胁定位），并不要求确凿识别攻击者。但是在网空，即使是针对攻击计算机的纯防卫性措施，也可能对全球网空基础设施造成严重的、意料不到的雪崩式后果，更不用说一旦反击伤及无辜，会出现什么样的政治梦魇。

第四，将网空中的作战能力和打击目标匹配，涉及若干独特的问题。进攻性行动可能要求有精确作战能力，是以避免严重的附带损伤。防卫性态势（或危机响应）则可能

需要使用强大的反击和威慑能力来应对各种攻击者，重点放在构建宽广的防火墙，而不是定点打击能力。

第五，评估网空领域的潜在附带损伤是一项艰巨的工作，需要大量的情报，而网络互联性及系统冗余则要求有精细的规划。目前，我们没有评估网空目标选定之附带损伤的正式方法。[39] 套用武力打击中的评估程序可能产生问题，因为网空同时存在于物理层面和虚拟层面。

尽管网空目标的选定面临这些独特的挑战，JP 3-60 向网空军事行动策划者提供了充分的原则框架。[40] 不过对于网空作战而言，还是有改进和澄清的余地，尤其是在附带损伤评估及战斗损伤评估方面。[41]

几项建议

对目前网空目标选定指导原则的改进应该从下一版 JP 3-60 开始，这部未来新版文件的出版说明中必须声明：该作战准则的基本原理同样适用于新兴网空领域中的目标选定。此声明应起到两个作用，一是认可网空军事作战的重要性和独特性，二是确认这部文件中的作战目标选定原则具有普适性。

如上所述，JP 3-60 应该概括说明如何执行网空领域中的附带损伤和战斗损伤评估，也许可包括相应的战术 / 战技 / 战规，指导作战人员识别服务器上其他敌方或平民网站，或者追踪潜在的第二阶和第三阶效应及其可能的地理位置。实际上，由于大多数进攻性网空作战行动不会造成实体损害，JP 3-60 应该指导如何区分网空效应和网空损伤，给出判定网空附带效应的方法指导。这种区分应该使用“武力打击损伤”（网空作战行动导致的实体损毁或破坏）作为评判标准。任何未导致实体损毁的网空作战行动只会产生“效应”。策划者只应该对那些实体损毁了预定目标和误伤了其它目标的行动进行作战损伤评估，而对其他网空作战行动则做附带效应评估。

未来的新版 JP 3-60 应该包含一个关于网空领域复杂性的简短章节，可借鉴 AFDD 3-12 的“理解网空”和“作战环境”这两个章节作为现成的范本。[42] 这个简短论述的目的是让联合作战策划者知道，在做网空中具体和时敏目标选定时，需要考虑一些独特的和额外的因素。

另外，新版 JP 3-60 应该注意把进攻性和防卫性网空目标选定加以区别，尤其是要把握好追究攻击来源的确凿度，为确凿识别网空目标提供条件。如果是为进攻性网空作战行动（例如：计算机网络攻击）做策划，那么对计算机网络、网站、角色或基础设施的攻击来源追究更应该尽可能准确判定（真正的确凿识别），是以符合战争法的区分原则。如果作战的目的是击退敌方对我方的计算机攻击或迫近攻击，则按自卫原则，此时网空联合作战策划者可有较大的灵活性。在网空防卫行动的策划中，不妨运用一种敌对来源追究准确程度递降尺度，从而做到追究的准确程度与自卫反击措施所产生的预期损伤或效应程度基本对应。在尺度的高端，反击措施打击范围大，持续时间长，强度高，可能导致巨大的火力打击损毁，因而需要几乎确凿判定攻击来源之后才可行动。在尺度的低端，是纯技术性的——甚至只是自动响应的——机制自卫行动，并非真正使用武力，因而不需要详细追究攻击来源。这类网空“反制措施”包括检测、消毒、隔离检疫，或者只是设置屏障阻挡恶意通讯和断开攻击计算机与受攻击计算机之间的网络连接。

最后，新版 JP 3-60 应该解说敌方网空重心概念和网空联合作战区域概念。敌方的网空存在包括计算机、信息系统、硬件、在线角色等等，它们可能与敌方的实体重心不在同一个地理位置。作战策划者一旦识别网空重心（那是一个关键点，是敌方网空作战行动的力量源），就可以选定该目标。联合特遣部队指挥官可以建立网空联合作战行动区域的实体界线和虚拟界线，并且具体指示该区域的目标选定交战规则。用这种方法分隔网空，可以尽量减少潜在的雪崩式附带损伤和效应。

总之，JP 3-60 向网空联合作战部队充分提供了适用于网空领域的目标选定原则指导。如果这部文件能够稍加修改，并加入针对具体领域的指导说明，将对网空战士更加有用。♣

注释:

1. Wesley R. Andrues,“What U.S. Cyber Command Must Do”[美国网空司令部必须做什么], Joint Force Quarterly 59 (4th Quarter 2010): 117, http://www.ndu.edu/press/lib/images/jfq-59/JFQ59_115-120_Andrues.pdf.
2. Tom Gjelten,“Extending the Law of War to Cyberspace”[将战争法延伸到网空], National Public Radio Online, 22 September 2010, http://www.npr.org/templates/story/story.php?storyId=130023318. 在本文英文中，“Kinetic”指与传统战争相关的物理或武力打击行动。
3. DOD Directive (DODD) 2311.01E, DOD Law of War Program [国防部战争法计划], 9 May 2006 (incorporating change 1, 15 November 2010), 2, http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf.
4. 本文所用的术语“原则”有下列含义：(1) 在“目标选定”语境中，指主要信念、公认的最佳方法以及可产生预期作战效应的军事指导方针；(2) 在法律语境中，指核心法律信条。联合作战准则将这两种含义混合使用，但本文却将它们分开，以凸显传统的军事武力打击行动和潜在的网空作战行动之间的某些区别。
5. Joint Publication (JP) 3-60, Joint Targeting [联合作战准则 JP 3-60：联合目标选定], 13 April 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf.
6. JP 1, Doctrine for the Armed Forces of the United States [JP 1：美国武装部队作战准则], 2 May 2007 (incorporating change 1, 20 March 2009), I-1, I-21, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.
7. 战争法是“国际公法的一个分支,包含文明国家遵循的许多法规和原则,藉以规范公开战争内在或附带的行为事项。”参看 Black's Law Dictionary [布莱克法律辞典], 6th ed. (St. Paul, MN: West Publishing, 1990), 1583.
8. International Conferences (The Hague), Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land [海牙第四公约:陆战法规和惯例公约，以及附件:陆战法规和惯例章程], 18 October 1907, http://www.icrc.org/ihl.nsf/full/195; 另参看 Hague Convention (III) Relative to the Opening of Hostilities [海牙第三公约：关于战争开始的公约], 18 October 1907, http:// www.icrc.org/ihl.nsf/FULL/190?OpenDocument; 另参看 Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land [海牙第五公约：中立国和人民在陆战中的权利和义务公约], 18 October 1907, http://www.icrc.org/ihl.nsf /FULL/200; 另参看 Geneva Conventions I-IV [日内瓦公约 I-IV], 12 August 1949, International Committee of the Red Cross, http://www.icrc.org/eng/war-and-law/treaties -customary-law/geneva-conventions/index.jsp.
9. Charter of the United Nations, Article 2(4) [联合国宪章，第 2(4) 条], 26 June 1945, http://www.un.org/en/documents/charter /chapter1.shtml.
10. 见注释 8 中海牙第四公约，第 23(g) 条。
11. 见注释 8 中海牙第四公约，第 23(e) 条。
12. United Nations General Assembly Resolution 2444 (XXIII) [联合国大会第 2444 (XXIII) 号决议], 19 December 1968, as cited in International Committee of the Red Cross, Weapons That May Cause Unnecessary Suffering or Have Indiscriminate Effects: Report on the Work of Experts [由国际红十字会引用于：可能引起不必要痛苦或具有滥杀滥伤作用的武器：

专家工作报告], (Geneva, Switzerland: International Committee of the Red Cross, 1973), 13, http://www.loc.gov/rr/frd/Military _Law/pdf/RC-Weapons.pdf.

13. 见注释 8 中日内瓦公约 IV，第 4 条和第 27 条。

14. Judge Advocate Genera's School, Air Force Operations and the Law: A Guide for Air, Space, and Cyber Forces [空军作战行动和法律：天空、太空和网空部队指南], 2nd ed. (Maxwell AFB, AL: Judge Advocate General's School, 2009), 21, http://www.afjag.af.mil/shared/media/document/AFD-100510-059.pdf; 另参看《海牙第四公约》序言："住民与交战团体仍在国际法原则之保护与管辖之下，这些原则是在文明国家间，从人道法则和公共道德规则的习惯所建立起来的。"

15. JP 1-02, Department of Defense Dictionary of Military and Associated Terms [JP 1-02：国防部军语词典], 8 November 2010 (as amended through 15 May 2011), 362, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

16. 请参看 MAJ Keith E. Puls, ed., Law of War Handbook [战争法手册], (Charlottesville, VA: International and Operational Law Department, Judge Advocate General's Legal Center and School, US Army, 2005), 139-42, http://www.loc.gov/rr/frd/Military_Law/pdf/law-war-handbook-2005.pdf.

17. Air Force Doctrine Document (AFDD) 2-1.9, Targeting [空军作战准则 AFDD 2-1.9：目标选定], 8 June 2006, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-60.pdf.

18. 网空是一个全球性领域。请参看 JP 1, Doctrine for the Armed Forces of the United States, GL-7 [JP 1：美国武装部队作战准则，GL-7 节]; 另参看 Cheryl Pellerin,"Cyberspace Is the New Domain of Warfare"[网空是新的战争领域], U.S. Air Force AIM Points, 18 October 2010, http://aimpoints.hq.af.mil/display.cfm?id=41748&printer=no.

19. Maj Steve Smart,"Warfare in the Cyberspace Domain"[网空领域的战争], (thesis, Air Command and Staff College, Maxwell AFB, AL, 2010), 3. 这是笔者提议的"网空领域"新定义。将网空描述为一个作战领域颇具敏感性和争议性。请参看非保密的"White House Guidance Regarding the Use of 'Domain' in Unclassified Documents and Public Statements"[白宫关于在非保密文件和公告中使用'领域'一词的指导意见], 14 March 2011. (FOUO)

20. Christina Mackenzie,"Do No Harm"[不可伤害], Aviation Week: Defense Technology International—Cyber War Issue, September 2010, 37.

21. 同上。

22. Michael Dumiak,"Casus Belli"[宣战原因], Aviation Week: Defense Technology International—Cyber War Issue, September 2010, 31.

23. 主管政策的国防部副部长和参谋长联席会议主席将修订信息作战政策和作战准则文件，以指导如何将信息作战整合入军事作战行动,而不再强调信息作战的核心能力。这个转变标志着向网空作战行动"主流化"迈出重要的一步。请参看 Robert Gates, secretary of defense, memorandum, subject: Strategic Communication and Information Operations in the DOD [国防部长备忘录，主题：国防部的战略通讯和信息作战], 25 January 2011, http://www.carlisle.army.mil/dime/documents/Strategic%20Communication%20&%20IO%20Memo%2025%20Jan2021.Pdf.

24. JP 3-13, Information Operations [JP 3-13：信息作战], 13 February 2006, I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. 信息作战的新定义是"在军事行动中综合使用信息相关作战能力，与其他作战行动协同配合，以期影响、干扰、破坏或剥夺敌方或潜在敌方的决策机能，同时保护己方的决策机能。"另参看注释 23 中国防部长备忘录，第 2 页。

25. 见注释 24，第 II-1 页。

26. 请参看 JP 3-13.1, Electronic Warfare [JP 3-13.1：电子战], 25 January 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf; 另参看 JP 3-13.2, Psychological Operations [JP 3-13.2：心理作战], 7 January 2010, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_2.pdf.

27. 这不是说国防部没有提供网空作战指导，而是想指出，目前几乎没有对作战人员有用的引导。请参看 DODD 3600.01, Information Operations (IO) [信息作战], 14 August 2006, http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf; 另参看 DODD O-8530.1, Computer Network Defense (CND) [计算机网络防卫], 8 January 2001.

28. AFDD 3-12, Cyberspace Operations [网空作战], 15 July 2010, 2, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf.

29. 同上，第 16-20 页及第 22-28 页。

30. 见注释 28。

31. 美国网空司令部正在逐步确定其在网空领域的各种作用和使命，最终建立起“统一的愿景”。参看 Mark V. Schanz, “Cyber Command Working Out Roles and Relationships”[网空司令部正在逐步确定其作用和关系], Daily Report, airforce-magazine.com, 21 October 2010, http://www.airforce-magazine.com/DRArchive/Pages/default.aspx. 还有，科罗拉多州巴克利空军基地第 460 太空联队完成了第一次专注网空问题的演习，参看 MSgt J. LaVoie, “A First-of-Its-Kind Cyber Exercise”[有史第一次网空作战演习], Daily Report, airforce-magazine.com, 29 October 2010, http://www.airforce-magazine.com/DRArchive/Pages/default.aspx.

32. 见注释 5，第 II-3 页。

33. 见注释 5，第 II-3 页。

34. Martin C. Libicki, Cyberdeterrence and Cyberwar [网空威慑和网空战], (Santa Monica, CA: RAND Corporation, 2009), 11, http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

35. Timothy L. Thomas, Cyber Silhouettes [网空概述], (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), 19.

36. 见注释 5，第 III-2 页。

37. 见注释 5，第 I-2 页。

38. 一场政策辩论正在网空专家和政府领导人之间展开，焦点是在危机应对过程中，对所有网空作战行动要求确凿识别攻击来源的必要性及可行性。

39. United States Joint Forces Command, Joint Fires and Targeting Handbook [联合作战火力和目标选定手册], (Suffolk, VA: Joint Warfighting Center, Joint Doctrine; Norfolk, VA: Joint Capability Development, Joint Integrated Fires, 19 October 2007), http://www.dtic.mil/doctrine/doctrine/jwfc/jntfiretar_hdbk.pdf.

40. Kevin Beeker 少校（美国网空司令部代理 J2T）和 Dustin Dargis 军士长（美国网空司令部）与作者访谈记录，2010 年 11 月 2-4 日。

41. 同上。

42. 见注释 28，第 2-5 页。

史蒂文·斯马特，美国空军少校（Maj Steven J. Smart, USAF），约翰布朗大学理学士，空军大学文科硕士，Gonzaga 大学法学院法学博士，现在国防部美国空军总部任军法署总监办公室战略通信主任。此前他在美国网空司令部及其前身机构联合职能部队司令部——网络战 / 全球网络作战联合特遣部队担任目标选定与作战法律总顾问，就网空军事行动规划中有关战争法、交战规则、及国际法问题向司令官和跨机构联合特遣部队提供咨询。他是目标选定与网空攻击团队、危机与应急规划小组和网空响应规划人员的首席法律顾问。斯马特少校在其军旅生涯中还担任过军法检察官、辩护律师及采购与环境法律师，也曾担任军法署人事副主任发挥领导作用。斯马特少校是空军指挥参谋学院 2011 届毕业生，其间因对推进信息作战、包括影响战、电子战及网络作战的贡献而获得 Michael Hayden 中将研究奖。