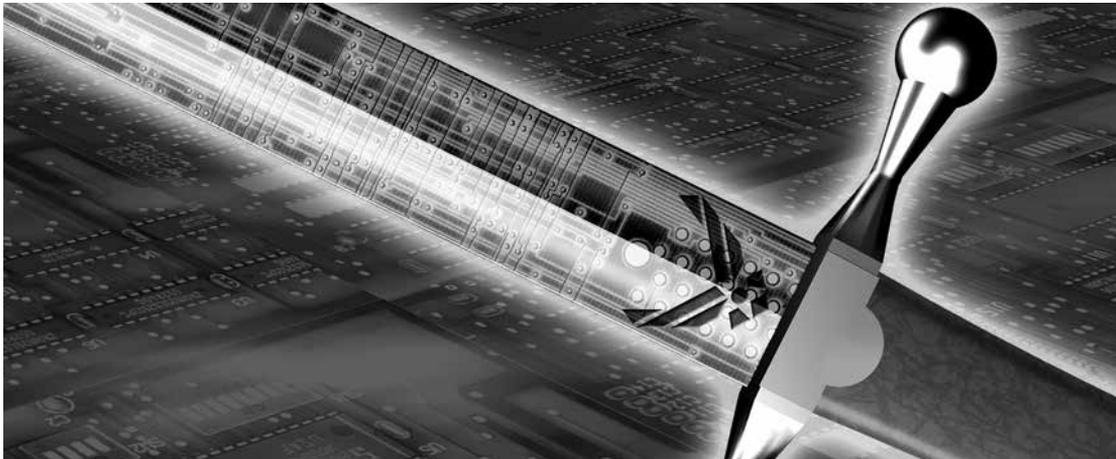


# 正式命名网空武器系统的意义所在

## The Importance of Designating Cyberspace Weapon Systems

罗伯特·J·斯金纳, 美国空军准将 (Brig Gen Robert J. Skinner, USAF)



在美军联合出版物 JP 1-02《国防部军语词典》中,武器系统的定义是“一种或多种武器与所有相关设备、材料、服务、人员,以及运载和部署(如适用)方式结合而形成的自我完备的整体。”<sup>1</sup> 当人们谈及美国空军和武器系统时,最先想到的可能是 B-2“幽灵”隐形轰炸机, F-15E“攻击鹰”战斗机,或 F-16“战隼”战斗机;进一步,“民兵-III”导弹、全球定位系统,或 KC-135“同温层油船”空中加油机等也可能成为讨论的内容。因为毕竟,空军的使命是在天空、太空和网空中飞行、战斗和制胜。属于天空和太空领域的这些资产,都是久经考验、名副其实的武器系统。现在,在这一长列武器系统清单中,空军又增添了支持网络空间作战的新武器系统,“运用这些网空能力,着重在网空、从网空或通过网空实现作战目的。”这些系统的独特之处在于它们离不开最新的作战领域即网空,而“网空是一个信息环境中的全球领域,它由相互依赖的信息技术

AOC = 空天作战中心

基础设施网络和内宿数据组成,包括互联网、通信网络、计算机系统,以及嵌入式处理器和控制器。”<sup>2</sup>

2013年3月24日,空军参谋长批准了空军太空司令部属下六种网空武器系统的正式命名,指定太空司令部负责组织这些武器系统,装备到部队,并训练使用这些系统的人员。“全球到达,全球力量,全球警戒”作为空军的使命,过去覆盖天空和太空,现在随着以下六种武器系统的正式命名而进一步覆盖网空:

- ACD — 空军网空防御武器系统
- CDA — 网空防御分析武器系统
- CVA/Hunter — 网空安全漏洞评估/寻猎武器系统
- AFINC — 空军内联网控制武器系统
- CSCS — 空军网空安全和控制武器系统
- C3MS — 网空指挥控制任务武器系统

这些名称就能力而言，可能含有某些重复，但组成这些武器系统的人员和设备则各自执行特定的使命，并互为补充。所有这些武器系统都是为着提供网空能力和确保网空安全，保障其他使命和保护关键信息，同时保卫我们的网络抵抗攻击。在思考这一系列网空武器系统的能力时，不妨对比空军军事空运武器系统，如C-5、C-17、C-130等，它们都是运输机，但每一种飞机在整体空中机动使命中发挥着独特的作用。正如这些武器平台存在明显区别一样，网空武器系统也按各自作战能力的不同而各异。它们的使命范围可能会有重叠，但其互补的性质与我们的空运平台系列极为相似——相辅相成，提供完整能力。

据美国麦迪安网络安全公司今年早些时候在一份题为“先进持续渗透攻击（APT）1：揭露中国一家网络间谍单位”的报告所披露，中国频繁对美国网络开展攻击，凸显出我空军和国家发展网空能力已迫在眉睫，是以保卫这个关键领域，确保信息优势。这份报告论述了持续渗透威胁，指出“我们对数百个调查中的大量细节所做的分析让我们确信，从事这些活动的团体地点主要在中国，而且中国政府对此心知肚明……我们分析的结论是，APT 1可能是政府支持的、持续时间最长的中国网络威胁执行单位之一。”麦迪安公司关于APT 1的报告仅仅对中国20多个APT单位中的一个进行了详细揭露，跟踪到这支部队在过去7年中向近150家受害者发动网络攻击，窃取了数百万亿字节的数据信息。<sup>3</sup>不过，本文的讨论显然并不局限于任何特定的对手。形形色色的侵略者盘踞在网空领域中，既有躲在自家房屋地下室单枪独干的个人，也有多人凑合的团体，还有主权国家。他们的意图也多种多样，间谍、窃取

知识产权、组织犯罪、盗窃身份信息、军事行动等等，不一而足。

本文对以上六种武器系统逐一描述，检视其历史和独特能力，并介绍运作此每一武器系统的具体部队单位。然后本文探讨把这些能力归为“武器系统”的重要意义，论述这些系统将如何直接对付我们今天面对的种种威胁。不过在此之前，本文首先提供一幅背景画面，帮助大家理解武器系统的能力和这些武器系统针对敌人的应用。

假设你是一名坐在一个主要司令部内计算机桌前的政府文职人员，刚收到一封有关自动削减财政拨款和全体员工可能无薪休假政府关闭的提前招呼邮件。邮件中有一个“详情请见……”的网络链接。你试图打开这个链接，但收到一个出错提示；你再次尝试，结果一样。于是你一忘了之而继续做你的工作，却没有意识到，这个链接已经把你的工作计算机引向一个恶意网络服务器，通过下载一套恶意程序，使对手能掌控你的计算机。怎么会发生这种事呢，为什么有人盯住你呢？事实上，要弄清楚并不难。还记得在限制出差的通知发出之前的几个月，你曾参加过什么研讨会吗？对手从会议的签到簿上窃取了你的电子信箱地址，会议的其他参办单位也可以分享这份签到簿的信息。但为什么特别青睐你呢？原来对手意识到你从事某种特定专业且能接触到有价值的信息，属于“目标丰富环境”类。在这类人中，只要有一个人点击了对手在此邮件中设置的链接，就会触发一系列的恶意行动。对手没有在你的计算机中留下任何问题痕迹，但是他现在能畅通无阻地接触那些非机密但有用的信息。

空军如何对付这种侵入？实际上，防御“钓鱼”攻击的最佳办法是教育计算机使用者

提高警惕。然而,对手的攻击手段越来越复杂,有时几乎无法辨认。美军各军种都有网空部队负责网络防护。具体到本案,空军通过网络流量监控手段怀疑你的工作计算机被侵入,于是上报。网络运作单位发现非同寻常数量的数据流从你的基地流向另一个国家的网址,于是通知第 624 作战中心,包括空军特别调查局的人员,然后该中心开始实施指挥控制并会同执法部门一道处理这次事件。网空取证分析专家被派去调查此案,不仅要找到“被感染”的设备,还要确定对手如何潜入空军网络系统。网空指挥控制部门则派网空作战风险评估人员勘查事态,确定数据泄漏种类和程度并评估损失。空军的计算机应急响应分队检查该基地的计算机和其他硬件,找出攻击方渗入我军计算机系统的准确途径及方法,据此制定(并分享)专门对抗这种威胁的防御行动,并作为编写新战术/战技/战规的参照。进一步,应急响应分队据此修补空军所有的工作计算机,以应对未来使用同类技术的攻击企图;应急响应分队还支援该基地开展网络清理和加固。在概略介绍了这次远程攻击后,让我们更深入讨论上述网空武器系统和执行相应使命的部队单位。

## 空军网空防御武器系统

空军网空防御(ACD)武器系统阻止、侦测和回应外部对非机密和机密网络的侵入并提供取证分析。ACD 武器系统由德州圣安东尼奥-拉克兰联合基地第 33 网络战中队以及罗德岛州匡塞特空军国民警卫队基地第 102 网络战中队运作,支援计算机应急响应分队开展其工作。该武器系统的各操作团队由一名网空勤务组长、一名副组长、一名网空作战控制员和 33 名网空分析员组成,他们进一步获得其他人员的支援。

ACD 武器系统从应急响应分队发展而来,应急响应分队的主要责任是协调原空军信息作战中心的技术部门评估、分析、降低计算机安全事故和薄弱环节。现在,ACD 武器系统连续监控和防卫空军非机密和机密网络,在以下 4 个任务领域运作:

1. 事故预防:保护空军网络抵抗现有的和新现的恶意逻辑攻击,评估和化解软件和硬件的已知漏洞。

2. 事故侦测:对空军机密和非机密网络进行监控,识别和调查反常活动,确定对网络造成的问题和威胁,监控网络传感器发出的实时警报,对传感器报告的历史流量进行深入探究。

3. 事故反应:确定侵入的范围程度,制定化解威胁的行动方案,确定并实施反应行动。

4. 计算机取证分析:开展深入分析来确定来自认定事件和可疑活动的威胁,评估损失,支援事故反应程序,捕捉各种“探哨”代码造成的破坏,逆向设计代码以确定对网络/系统的影响。

## 网空防御分析武器系统

网空防御分析(CDA)武器系统实施网空防御作战,对从己方非保密系统如计算机网络、电话、电子邮件,以及美国空军部队网站发布的敏感信息进行监控、搜集、分析和报告。CDA 武器系统对于防止危害作战安全的信息泄漏至关重要。空军三支现役部队(第 68 网络战中队、第 352 网络战中队和第 352 网络战中队第一支队)和两支后备役部队(第 860 网络战飞行中队和第 960 网络战飞行中队)运作这个武器系统,他们分别位

于德州圣安东尼奥 - 拉克兰联合基地、夏威夷州珍珠港 - 希卡姆联合基地、德国拉姆施泰因空军基地，以及内布拉斯加州奥弗特空军基地。该武器系统的各操作团队由一名网空作战控制员和三名网空防御分析员组成，他们进一步获得其他人员的支援。

CDA 武器系统有两个衍生版本，但都旨在监视、搜集、分析和报告经非保密通信系统传送的空军官方信息，决定其中是否包含敏感或保密内容。该武器系统根据需把发现的可疑泄漏报告给战地指挥官、作战安全监控员或其他人员，以决定潜在的影响和作战调整。第二个版本根据网络侵入的情况，提供更多功能来进行信息损害评估，同时对空军非保密网站进行评估。第二个版本只由第 68 网络战中队操作。

CDA 武器系统在下列 6 个任务领域开展监控和 / 或评估：

1. 电话语音：监控和评估空军非保密语音网络。

2. 无线电频率：监控和评估空军的 VHF, UHF, FM, HF 和 SHF 频带的通信（移动电话、陆地移动无线电和无线局域网）。

3. 电子邮件：监控和评估在空军网中通过的空军非保密电子邮件的流量。

4. 网基能力：监控和评估源自空军网、但上传至非由国防部或联邦政府所有、操作或控制的公开网站中的信息。

5. 网空作战风险评估（由第 68 网空战中队操作的该武器系统第二版本发现的风险）：评估由于侵入空军网而受损的数据，以决定因数据流失对相关作战产生的影响。

6. 网络风险评估（由第 68 网空战中队操作的该武器系统第二版本发现的风险）：评估上传至由空军所有、租用或操作的非保密的公开和私人网址上的信息，以降低这些信息被敌人利用的风险，减少对空军和联合作战的任何不利影响。

## 网空安全漏洞评估/寻猎武器系统

网空安全漏洞评估（CVA）/ 寻猎武器系统对空军和国防部网络和系统进行安全漏洞、合规、防御状态和非技术评估、最佳做法审核、渗透试验，以及寻猎行动。寻猎行动在于确认并消除威胁，以为执行各种既定使命提供保障。此武器系统可对全球各站点计算机远程访问或现场访问执行防御任务。CVA/ 寻猎武器系统由一支现役部队、即德州圣安东尼奥 - 拉克兰联合基地的第 92 信息战中队，和一支国民警卫队部队、即华盛顿州路易斯 - 麦科德联合基地的第 262 网络战中队联合运作。此外，还有两个国民警卫队单位正在向该使命过渡，他们是位于华盛顿州穆雷营的第 143 信息战中队和位于加州塞普尔维达空军国民警卫队站的第 261 网络战中队。此武器系统的各操作团队由一名网空勤务组长、1-4 名网空操作员、1-4 名网空分析员组成。还有其他人员对这些团队提供支援。CVA/ 寻猎武器系统由原空军信息作战中心开发，于 2009 年部署在第 688 信息作战联队。

纵观历史，在“持久自由”和“伊拉克自由”行动期间，安全漏洞评估对保证使命成功发挥了重要作用。CVA 现在继续提供这一关键能力。此外，这个武器系统现在作为寻猎行动的第一阶段。寻猎使命源自防御网络战略的变革，从“设法保卫整个网络”变为“提供网络使命保证”，经此变革而提供坚固纵深防御的保障能力。从 2010 年 11 月以

来，CVA/ 寻猎武器系统的原型系统已参与过真实世界的作战行动。该武器系统在 2013 年 6 月达到初始作战能力。

CVA/ 寻猎武器系统旨在找出漏洞，向指挥官提供关键使命网络中现存漏洞风险的整体评估。它在功能上分为三种平台，一是便携式平台，由操作人员用于现场访问或远程访问以执行评估；二是可部署的传感器平台，用作搜集和分析数据；三是军营基地平台，用于为远程访问和高级分析、测试、培训和归档提供所需的连接能力。具体而言，寻猎使命侧重寻找、修补、跟踪、锁定、交战和评估先进的持续威胁。

在主动交战中，CVA/ 寻猎武器系统和己方网络防御部队协同，向第 24 空军和空军网空及作战指挥官提供一种可移动的精确保护能力，用以识别、追踪并化解网空威胁。它可以装备各种模块化载荷，包括为特定防御使命而优化的载荷和为在网空生成具体效果而设计的载荷。运作 CVA/ 寻猎武器系统的每个团队能进行一系列的评估，包括安全漏洞分析、合规评估、渗透试验等，以及对这些评估派生的数据进行分析 and 特征归纳。此武器系统的有效荷载由商用及政府现成硬软件组成，包括配置了定制的漏洞评估工具 LINUX 和视窗操作系统。

## 空军内联网控制武器系统

空军内联网控制武器系统 (AFINC) 是空军信息网络的边界和入口顶级控制门关，确保所有外部和基地间数据交流通过标准的中央管理门关传送。AFINC 武器系统由 16 个门关套件和两个综合管理套件组成，由阿拉巴马州蒙哥马利市甘特附属基地第 26 网络战中队运作，AFINC 的各操作团队由一名勤务

组长、一名副组长、一名网空作战组长、两名作战控制员、两名网空操作员和三名事件控制员组成，他们进一步获得其他人员的支援。

AFINC 武器系统取代并整合区域管理的、散布的空军网络，将这些网络并入一个集中管理的访问入口，从而控制进入空军信息网的访问流量。它提供以网络为中心的服务，保障核心服务，使整个网络的防御作战有更大的灵活性。AFINC 武器系统通过以下四个任务领域整合网络作战和防御：

1. 纵深防御：通过整合门关和边界装置实现全局性分层防御方式，从而增强网络的韧性和使命保证。

2. 先机防御：持续监控空军网络流量，关注其反应时间、进出流量及性能表现，确保及时传送关键信息。

3. 网络标准化：制定并维护标准和政策，保护网络、系统和数据库，减少维护的复杂性、停运期、成本和培训要求。

4. 态势感知：提供网络数据流、流量模式、利用率，以及对历史流量的深度研究，从中发现对非正常事件的解决线索。

## 空军网空安全和控制武器系统

空军网空安全和控制系统武器系统 (CSCS) 提供全时、全天候网络作战和管理职能，为空军机密和非机密网络内的关键全局服务提供保障。它还支持空军网络内的防御作战。CSCS 武器系统由两个现役网络战中队、一个空军国民警卫队网络安全中队，以及与现役中队对应的两个空军后备役司令部网络战辅助中队共同运作。其中第 83 和第 860 网络战中队驻扎弗吉尼亚州兰利空军基

地；第 561 和第 960 网络战中队驻扎科罗拉多州彼得森空军基地；第 299 网络作战安全中队驻扎堪萨斯州麦康奈尔空军基地。该武器系统的各操作团队由一名网空勤务组长、一名网空作战控制员、一个作战组（实施边界、基础设施、网络防御、网络节点、以及漏洞管理功能），以及一个全局服务单位（提供短信发送和协作、目录和密码认证、存储和虚拟化管理，以及监控管理）组成。还有其他人员对这些团队提供支援。

CSCS 武器系统源自过去的网络整合努力，经此努力把各大司令部的众多网络整合到中央管理和控制的网络中，归三个整合的网络作战及安全中心管理。2007 年，空军成立了两个现役网络战中队来提供这些功能；空军国民警卫队的网络战安全中队则为警卫队的基地和单位提供相同的功能。

CSCS 武器系统执行网络运行和故障处理活动，旨在维持作战网络正常运行。其操作人员监控和评估实时网络事件并做出反应，识别异常活动并分析特征，以及根据上级部门指示采取适当的反应行动。该武器系统支援对进出空军基地层级的飞地网络进行实时流量过滤，并屏蔽可疑的软件。CSCS 操作人员持续不断地与基地层级网络控制中心及通信节点进行协调，解决网络中的问题。其他关键的能力包括漏洞识别和修复，以及对进出空军基地层级的飞地网络的流量控制和安全。CSCS 还提供空军全局性服务，包括短信发送和协作、存储，以及建立受控环境以容纳基于网络的系统从而支援空军实施各种具体使命。

## 网空指挥控制任务武器系统

网空指挥控制任务武器系统（C3MS）的作用是保障空军实施各种使命，它指挥空军其他网空武器系统同步行动，形成战役层次效果，支援在全球行动的各作战指挥官。此武器系统对空军各网络部队、网络和使命系统提供战役层次 C2 及态势感知，保障第 24 空军司令正确制定和发送网空行动战略和计划，司令官进一步实施并评估这些计划的执行情况，以支援空军和联合作战将士。C3MS 武器系统由德州圣安东尼奥 - 拉克兰联合基地第 624 作战中心运作，各团队包括一名资深值班官、一名资深副值班官、一名网空防御警戒军官、一名网空进攻警戒军官、一名国防部信息网络警戒军官、三名网空防御作战控制员、三名网空进攻作战控制员、三名国防部信息网络作战控制员、一名网空效果计划员，一名网空作战战略官、一名网空情报分析员、一名网空作战评估分析员，以及一名网空作战报告单元分析员。还有其他人员对他们提供支援。C3MS 武器系统从传统的空军网络作战安全中心概念、人员和设备发展起来。在正式成立美军网空司令部和组建第 24 空军后，高层领导班子认识到需要建立战役层次的网空 C2 能力。

C3MS 作为空军的统一武器系统，提供对网空领域中空军部分的永久性全局态势感知、管理和控制。它确保网络进出畅通、使命保证，以及联合作战将士使用网络和信息处理系统在全球范围作战。该武器系统有五个主要的子任务领域：

1. 态势感知：融合来自各种传感器、数据库、武器系统和其他来源的数据，生成战役全局图，以获得并保持对己方、中立方及

可能对联合部队和空军构成威胁的各类活动的态势感知。

2. 情监侦 (ISR) 产品：将网空预兆和迹象、分析以及其他可行的情报产品整合为全局态势感知，保障其策划和实施。

3. 制定计划：利用态势感知制定长期和短期计划、具体战略和行动方案，策划网络进攻和防御作战以及国防部信息网络作战的实施。

4. 实施计划：利用行动计划生成并跟踪各种网空任务命令，运用所属和附属部队兵力来支援网空进攻和防御作战以及国防部信息网络作战。

5. 与其他 C2 节点整合：将空军产生的网络效果与各空天作战中心、美军网空司令部，以及其他 C2 节点相整合。

## 为什么需要命名网空武器系统？

如果我们的确希望把网空看作与天空、陆地、海洋和太空同等的作战领域，那么我们的思维必须从视通信为一种支援功能转变视网空为一个开展军事行动的作战领域。为了在网空有效地飞行、战斗、制胜，空军必须适当地组织、训练和装备网空作战专业部队。多年来，空军内各类部门一直按照自身需要添补人员和装备，经常沿循年尾花余钱的做法，逐渐发展成当前的空军网络即 AFNet 基础结构和系统。出于同样的原因，现在构成这六种武器系统的各组成部分，过去一直没有一个主要司令部牵头制定作战需求，或实施标准化训练，或有效管理设备生命周期及其资源配置。这种各自为阵的做法，几乎不可能提供使命保证，无法保障空军和联合作战界在网空作战的关键使命。演进到

AFNet 结构之后，空军已能够朝着近 20 年前提出的网络运行作战化和专业化的愿景迈开大步。空军太空司令部牵头做出努力，划分出这六种武器系统，推动网空运作向更加规范的做法发展。现在对这六种系统正式命名，有助于更好地管理和维持设备的生命周期，同时加快空军网空专业战士的思维转型，从通信或信息技术的心态转向作战心态，辅之以全面的作战使命资格训练、作战部队标准管理，以及标准化和评估计划（如适用），使网空作战常态化，就像太空和导弹作战一样。进一步，正式命名这些武器系统将有助于网空领域获得适当的战员配备和计划性资金分配，保证空军能在网空飞行、战斗，制胜。

国防部是经由武器系统的划分来管理天空、太空、陆地和海洋优势并安排资源配置。要想在网空领域创造效果和构建优势，最好的途径是采用同样的武器系统划分架构，以管理网空能力和配置资源。正如我们在其他作战领域所做的那样，网空武器系统能为空军提供将网空建设成作战化、常态化，以及最终标准化的途径。空军担当着确保、运行和保卫国防部信息网络中属于空军的部分，并肩负着在网空领域保卫空军和联合部队的使命。这些网空武器系统为空军设置了走向网络规范化常态化作战的通道，从而成功实现上述目标。

正式命名网空武器系统后，空军维持武器系统的整体过程中便生成一条专用于网空武器维护的资金分配线。空军因此可将这份资金的调配规范化，并相应制定这类武器系统维持与维护所依据的长期计划，可以更合理更高效地使用有限的资源，而不是象过去那样依赖没有定数的年终结余资金，不加协调地花费掉。规范资金程序是一条关键的原则，只有这样才能保证武器配置管理标准化，

才能保证空军内（在某些情况下整个联合作战界）的武器系统做到互通运作。通过部署 AFNet 空军网络，我们已经取得了这些效益，有效简化了对空军整体网络安全的保护，正在进行的标准化也使用户获得更好的使用体验。

正式命名网空武器系统后，能生成类似其他作战领域中所得到的各种好处——通过命名武器系统这种标准的空军机制来推动组织、训练、装备和战斗力建设。武器系统命名后，空军就能常态化管理相关的作战能力，并保证这些系统标准化和持久化，随时接受作战指挥官的调用。当太空司令部人员比较天空和太空领域的常态化过程时，他们体会到只有正式命名武器系统能达成理想的结局。获得命名的武器系统也许不能总是得到充足的资源来支撑，但肯定比没有获得命名时的状态要好。

此外，对网空武器系统正式命名，直接有助于太空司令部作为牵头整合单位行使网空作战核心职能，保障太空司令部满足空军第 10-9 号政策指令中规定的责任，并推进网空内各种平台的标准化过程。<sup>4</sup>

正式命名这些武器系统，也直接关系到向战术单位提供所需的资源和训练，以形成常态化运作。实现跨领域整合的关键，在于能否合理利用不同领域的作战能力，而生成独特和决定性的效果——如果获得充足的资源配置的话。正式命名网空武器系统将推动网空领域向正确的方向演变，以及和其他作战领域构成合理的关系——这一点极为重要，因为在现代战争中，网空连接所有领域。把网空作战能力提升到这个层次，空军就能满足国防部的网空作战战略，该战略要求“国防部将把网空作为一个作战领域来组织、训

练和装备部队，使国防部能全面利用网空的潜力。”将网空运作和使命常态化及作战化的所有努力，更有助于推动空军向联合信息环境架构、标准和程序发展。国防部、美国网空司令部和各军种在推行联合信息环境建设的同时，也在组建多支网空使命部队，以支持国家、作战司令部和军种各自对网空的需求。把这些能力正式命名为武器系统，就便于这些部队在网空、从网空、通过网空更好地支持国家和联合作战界。

## 网空领域的独特挑战

天空、陆地、海洋和太空，都是自然领域，无需我们规划和建造，只需我们制造出工具来利用。自然领域不需要任何维护，但网空不同，网空主要存在于由人类设计、制造和配置的设备之间，而设备会过时，会磨损，需要不断地维护。此外，我们构建网空的方式，对我们运作和保卫该领域的能力有着直接的影响。运作网空和保卫网空同等重要，仅此一点，就使网空有别于其他领域。我们必须不断地培养和照料这个领域，还需要不断创新，才能保持领先，才能引领网空技术的发展。

保卫网空的努力亦有其独特的挑战，因为对手能出其不意地从全球任何地点发动网络攻击。对洲际弹道导弹的威胁，我们至少具备能侦测到导弹发射的传感器，我们的部队可以根据发射地点和预警时间做些准备并做出反应。在网空，我们很难预警敌对攻击，没有时间做出反应准备。因此空军必须发展侦测这种攻击的能力，能防则防，若防卫不及则沉着反应，做到象其它作战领域那样。我们还必须为自身利益发展利用网空的工具。在现实世界中，也许我们永远做不到万无一失地保卫我们的网络——要想达到这样的境界，势必要求我们投入过多的安全努力，

而牺牲网空给我们其它所有使命带来的战斗力倍增的好处。换言之，如果我们把所有对手都逼退于外，就只能把我们自己闭锁于内。这里的关键在于找到一个平衡点，让我们既能有效地保卫自己的网络和依赖网络的各种使命免遭攻击，又能尽量利用网空对这些使命带来的好处。

进一步，网空对空军和联合作战界在其他领域开展作战来说必不可少。我们今日在战争中做的一切几乎都依赖网空，无论是向卫星和导弹提供遥测，还是在阿富汗控制我空军的行动，我们必须依赖网空才能实施在其他所有领域的作战。

网空武器系统获得正式命名之后，就要求得到资源保证，才能达到天空和太空武器系统的相同标准。这是一个更高的运作标准，其所需要的相应资金配额和人力配备，远比以往把网空领域作为一种简单的通信或信息技术支援功能要更多。如果资金和人力配备得不到保证，可能会对每个其他所有领域的未来作战造成灾难性的冲击。网空作战化不仅仅是为了让太空司令部合理地组织、训练和装备网空部队——它更是网空向真正作战领域发展的逻辑演变，也是对其他所有作战行动的关键保障。

## 空天作战中心获得命名的启示

在1990年代后期，空军命名“鹰猎者”空天作战中心（AOC）为武器系统，但几乎没有对其采购、维持或需求做出什么正式的规定来支撑其发展。当时的空军参谋长只不过是同意“你们去做吧。”当时的作战界感受到各种需求挑战，颇像我们现在管理网空武器系统面临的挑战一样。通过宣布AOC为武器系统，空军希望改变各编号空军自配

设备和人员的各自为阵的混乱状态，形成统一规范化。这种观点认识到，把AOC命名为武器系统之后，就能更好地训练AOC人员，在计划目标备忘录程序中更好地为这项计划辩护，并在某种程度上保护编号空军部队的参谋资源被挖走去填补AOC岗位。

事实上，AOC的资金分配历经多次裁减，设备的维护和现代化一直难以满足底线要求，AOC人力配置成为多次效率演练检查的目标，导致影响范围缩小。难怪作战界有许多人认为，AOC被列为武器系统对其发展并无什么帮助。

但是空军作战司令部却持不同的看法，他们认为，AOC在整个过渡过程中尽管一直面对严重的挑战，但其今天的状态要比15年前强很多，尤其是在人员训练方面。在佛罗里达州赫尔伯特基地，一个专用的正式训练单位建立了一份记录项目，制订了一个严谨的配置和变化管理程序，最终获得作战界的赞赏，承认在联合部队空中组成部队司令官的战术空中控制系统C2概念中，AOC具有皇冠明珠的地位。此外，分配到AOC工作不再被认为是航空技术等级军官结束军人生涯前的最后一站——与1990年代的普遍看法大不一样，那时候，如果去某支编号空军就任参谋或AOC岗位，被广泛认为是专业晋升无望的死亡之吻。

空军太空司令部不会让AOC经历的初痛阻止我们推进网空武器系统的理念。每一个项目（无论是战斗机、轰炸机或ISR），都面对过其份内的挑战，但如果没有设立为项目——没有获得命名而名不正言不顺——那么网空武器系统为求生存就不得不为着一点资金和人力配额而无休止地争取。而今把这些网空武器系统整合到空军大结构之中的时

候，我们或许能从当年建立 AOC 武器系统所面临的挑战中吸收一些教训，避免重蹈错误覆辙。

## 结束语

美国通过网空来开展其它作战领域的行动。事实上，现今战争的所有方面——从通信、精确导航和报时、攻击预警、ISR 到 C2 等等——都依赖网空。正式命名网空武器系统将有助于空军保证网空畅通无阻，并为依赖网空的其他关键武器系统和作战领域提供使

命保证。空军为网空武器系统定名，就等于给出承诺，保证网空建设将在计划和预算中获得应有的重视，能保持网空作战，支援网空使命团队，向联合信息环境发展。进一步，受核心武器系统支援的网空作战将提供更好的安全、性能、灵活性，以及非规范化环境所无法生成的整体能力。网空作战化不仅仅是为了让太空司令部合理地组织、训练和装备网空部队，而是网空向真正作战领域发展的逻辑演变，也是对其他所有作战领域的关键保障。♣

## 注释：

1. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms [ 联合出版物 JP 1-02 : 国防部军语辞典 ], 8 November 2010 (as amended through 15 June 2013), 303, [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).
2. Mandiant, APT1: Exposing One of China's Cyber Espionage Units [ 先进持续渗透攻击 (APT) 1 : 揭露中国一家网络间谍单位 ] ([Washington, DC: Mandiant, 2013]), [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf). APT1:
3. Air Force Policy Directive 10-9, Lead Command Designation and Responsibilities for Weapon Systems [ 空军政策指令 10-9 : 牵头司令部对武器系统的命名和责任 ], 8 March 2007, [http://static.e-publishing.af.mil/production/1/af\\_a3\\_5/publication/afpd10-9/afpd10-9.pdf](http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afpd10-9/afpd10-9.pdf).
4. Department of Defense, Department of Defense Strategy for Operating in Cyberspace [ 国防部网空作战战略 ], (Washington, DC: Department of Defense, July 2011), 5, <http://www.defense.gov/news/d20110714cyber.pdf>.



罗伯特·斯金纳，美国空军准将 (Brig Gen Robert J. Skinner, USAF)，帕克学院理学士，俄克拉荷马市立大学理科硕士，现任空军网空军副司令官，担当空军与美国网空司令部和国家安全局的首席联络官及个人代表职责，并协调空军网空军对国防部长办公室、国家情报总监、中央情报局及其它国家与国会网空利益相关方的支持运作行动。将军于 1989 年获授军官衔，是空军中队指挥官学院、指挥与总参学院、空军战争学院及武装部队工业学院的毕业生。在其军旅生涯中，他担任过联队、大队及多个中队指挥职位、若干战术和固定通信职位，及在联合参谋部、空军参谋部和编号空军的参谋任职。担任现职以前，斯金纳准将在驻科罗拉多州彼得森空军基地的空军太空司令部总部任总监察官，领导一个下辖三部门五分支、包括 70 名人员的机构，负责评估遍及世界 100 余场所的 300 多个空军太空司令部太空与网空单位的战备状况。