美军网络部队培训体系特点及存在问题

彭　强，周时娥
（战略支援部队信息工程大学　基础部，河南　郑州　450001）

摘　要：美军网络部队已形成一个规模庞大、种类繁多的培训体系。本文试对该体系的特点及存在的问题进行分析。美军网络部队培训体系针对不同人员呈现多级别、多层次的特点，强调军种培训与联合培训相结合，大力依托地方资源广泛开展军地合作，注重认证驱动型培训模式，基本能满足当前美军网络部队工作的需要。但是由于网络部队成立时间较短，其培训体系仍存在若干有待解决的问题，如培训缺少官方统一的定义和标准，培训内容重技术轻文化，一些培训欠缺选拔机制等。

关键词：美军；网络部队；培训
中图分类号：E251　　**文献标识码：**A　　**文章编号：**1672－8874（2019）02－0076－04

Characteristics and Problems of the Training System of US Cyber Operations Workforce

PENG Qiang, ZHOU Shi-e
(*Basic Education Department*, *SSF Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: This essay analyzes the characteristics and problems of the training system of US cyber forces, a system of large scale and diversity. The US Cyber Command has established a multilevel, complicated training system, catering to different ranks and types of cyber operations personnel. The training system emphasizes the combination of services' training and joint training, encourages military and civilian cooperation, and tends to adopt certificate-driven training mode. However, problems remain to be solved, such as lack of uniformity in terms and standards, insufficient training on foreign cultures, and lack of screening in some advanced training programs.

Key words: US military forces; cyber forces; training system

一、美军网络部队人员及工作岗位情况概述

从 2002 年美国组建第一支网络战部队，到 2009 年成立隶属美军战略司令部的网络司令部，美军网络部队已初步成型。根据美国国防部 2011 年 4 月提交国会国防委员会的《网络行动人事报告》，截至到 2009 财年，美军网络行动人员人数总计 163144 人（含军人、文职人员、承包商），占国防部人员的 5% 还多。其中，军人（含现役、预备役、国民警卫队）是网络部队人员的主力，占总人数的约 83%，而军人中士兵与士官约占 87%[1]。

关于网络部队具体的工作岗位如何分类和定义目前还没有专门的条令出台。2014 年，兰德公司的一份研究报告将美军网络部队的任务分为计算机网络进攻、计算机网络防御、计算机网络利用三大类[2]。2008 年，美国国土安全部的相关文件将网络部队人员按职能分为五大类：管理员与

收稿日期：2018－12－17
作者简介：彭　强（1981－），男，河南郑州人。战略支援部队信息工程大学基础部讲师，硕士，主要从事军事情报学研究。

技师、研发人员与工程师、分析师、军需与采购人员、培训与教育人员[3]。美国国防部于2011年在《网络行动人事报告》中介绍了在非网络攻击领域工作岗位的人数分布情况，其中从事网络操作与维护的人员占绝大多数（约89%），而从事信息安全与保障的人员（9%）和网络防御作战的人员（2%）所占比例较少[4]。

2011年，美国国防部在其《网络空间行动战略》中指出："稳固和发展一支网络人才大军是国防部战略成功的核心"[5]。美军对确保拥有足够的高水平网络人才十分重视，目前已形成一个种类繁多、规模庞大的培训体系。本文所谈论的美军网络部队的培训，包含美军网络司令部及其下属部队所有从事网络相关工作人员的培训，长期的培训包括学历教育、任职培训等，短期的培训包括培训班、研讨会、训练营、拓展教育活动、网络课程等，均在本文讨论范围之内。研究美军网络部队培训体系，有助于为我军相关培训体系的建设提供参考借鉴。

二、美军网络部队培训体系特点

（一）培训体系呈多级别、多层次特点

美军的网络部队培训种类繁多，培训对象包括士兵、士官、军官、文职人员等。针对不同职衔级别和能力层次，有不同的培训项目相对应，大致可以分为入门级、初级、中级、高级四个级别（如表1所示）。美军网络部队培训强调"长期学习"，培训机会贯穿整个职业生涯，使相关人员有不断继续学习深造的机会，同时满足不同岗位、不同级别人员的工作需要。

表1　各级别培训内容举例[6]

培训级别	举　例
入门级	* 主要针对入伍新兵，如空军2010年在其入伍基本训练中加入网络意识培训课程，教授基本的空军网络操作知识和网络安全意识培养。
初级	* 空军"网络空间培训"，针对初级军官，培训合格获得相关证书。 * 陆军"信息技术专业培训"，培训士兵安装操作信息系统设备。 * 海军"信息系统管理员培训"，培训海军网络系统应用技术。
中级	* 空军指挥参谋学院提供中级职业教育，其中开设有网络战课程，培训对象大多为少校军衔。 * 陆军"信息系统管理课程"，面向管理层人员。 * 海军"网络安全脆弱性技师课程"，培训对计算机操作系统脆弱性的识别和纠正技术，毕业有相关证书。
高级	* 美国国防大学信息资源管理学院（又称iCollege），针对网络部队高级领导人员开设有信息技术项目管理、信息技术政策等课程。 * 空军战争学院、海军战争学院和陆军战争学院等，开设有网络安全战略的培训，面向战略层面的领导层。 * 联邦首席信息官训练营（Federal CIO Boot Camp）等短期培训。

总的来说，初、中级培训以实践技术为主，高级培训侧重战略管理。培训对象的军衔等级也从入门级到高级依次升高，入门级主要针对入伍新兵或大一新生，初级培训面向士兵、士官、初级军官等，中级培训对象为中级军官，而高级培训通常面向准将及以上军衔。不少学院可以提供各个级别的培训，如美国国防大学信息资源管理学院就提供了适用于从少校到一星准将的培训课程[7]。大多数培训通过后都有某个职位的资格证书，学历教育的培训有学位证书。部分中高级培训有一定的选拔机制，选拔出有一定基础的受训者，将有潜力的学员向更高层次的培训输送。总的来说，美军已建成一套相对完整的覆盖各个层次的网络部队培训系统，基本能够满足"从士兵到将军"的不间断学习的需求。

（二）军种培训与联合培训相结合

美国陆军、海军、空军、海军陆战队都有针对各个层次的网络技术培训课程。在学历教育方

面，美国海军学院和空军学院于 2013 年专门开设了网络行动（Cyber Operation）专业。西点军校虽然没有开设相关专业，但是成立了网络研究中心（Cyber Research Center）。短期培训方面，各军种都有针对其军种具体作战任务的培训或实习机会，时长从几个月到两年不等。不过，各军种网络系统目前尚不兼容，各军种培训的网络人才往往未必能胜任联合作战中的网络作战。

为了适应联合作战的需要，美军除了各军种自己的网络技术培训机构外，还设有联合培训课程。其中，较为重要的是位于佛罗里达州科里海军基地的信息优势中心（Center for Information Dominance）设置的“联合网络分析课程”（Joint Cyber Analysis Course，JCAC）。该课程培训为期六个月，属于高级培训，培训目标是满足网络战联合防御的需求，内容涉及执行各种网络任务所需的技术。其最初是海军的一个培训课程，后来成为跨所有军种的网络人才培训课程。这一课程的门槛较高，对参训人员要进行选拔，要求其接受过军种的中级网络培训课程，在专业的网络领域有一定的工作经历，表现优秀且具备很大的发展潜力。需要特别指出的是，该课程内容的设置受到美国国家安全局的高度参与[8]。受训人员在完成该课程培训后，潜力较大的学员将派往美国国家安全局接受进一步的通常为期半年的实践培训。实践培训合格的，将签订额外的三年服役合同，防止培训后退伍造成军队损失。

（三）军方与地方广泛合作

除了国防部、各军种、美国国家安全局开设的培训项目，由于网络技术基本上是军用商用相通的，而军队资源有限，故依托地方学校和公司进行培训也是一个重要的手段。这类军地合作大概可分为三类方式。

第一类是与私人公司、非政府组织合作。美国一些 IT 行业的公司有雄厚的技术实力和高端的网络技术人才，与它们进行合作自然会有很大的收益。例如，位于乔治亚州的陆军信息技术学校（School of Information Technology，SIT）就与多家 IT 公司合作，其中不乏国际知名公司，如微软、Adobe、NetApp 等，主要是开展网络安全方面的培训[9]。另外，地方还有一些网络技术培训公司或民间组织，专门提供这类培训。比如，美国有一家非政府组织名为“从战士到网络战士”（Warrior to Cyber Warrior，W2CW），定期提供为期五个月左右的培训课程，采用网络课程和课堂教学相结合的方式。军方往往会为培训人员支付培训费用。

第二类合作方式是与地方大学合作，在地方大学建立专门面向军队网络作战的培训机构。这种方式的合作目前在美国非常广泛。其中，规模最大的是美国于 1999 年启动的旨在进行信息安全保障培训和研究的“学术卓越中心”（Center of Academic Excellence，CAE）的建设。这类教育培训中心起初只有 7 所，随后迅速发展，截至到 2011 年已多达 117 所，学制分为两年制和四年制两种。绝大多数都设在地方院校，其中不乏世界知名学院如普林斯顿大学等；而军事院校只有六所设有该培训中心，如西点军校、国防大学、海军研究生院等。此外，还有与地方大学合作开办短期的培训班、研修班的模式。例如，2008 年美国国防部与内布拉斯加大学合作，成立了一年一度的国际网络防御研修班（International Cyber Defense Workshop），面向本国和来自盟国的军事人员，为期通常几个星期，培训如何发现、预防和补救网络安全漏洞[10]。

第三类是部队资助有潜力的网络工作人员去地方大学相关专业进修，学习地方大学已开设的网络技术课程。这种方式较为灵活，主要针对零星人员，属于一种辅助手段。不过，与地方合作也有不足之处。受法律等因素制约，地方企业和院校无法提供网络攻击行动（如黑客技术）方面的培训，因此主要提供的是信息防御方面的课程。

（四）注重认证驱动型培训

为了更贴近部队工作实际，同时激发部队人员的学习动力，美国网络部队有很多培训是专门针对某项网络技术证书的，针对性较强，帮助学员通过部队或地方相关认证考试，从而获得在某个岗位工作的资格证书。如前文提到的空军网络空间培训，初级军官参加该培训合格后获得“Security +”资格认证，可以胜任相关级别工作。美军关于网络战相关岗位的证书要求有详细的规定。证书从内容上大致分为信息安全保障技术、信息安全保障管理、信息安全保障设计师与工程师、计算机网络防御服务等几大类，每种资格证都分有等级，有些工作岗位不止需要一种证书。

此外，任务驱动型培训也是美军网络部队常见的一类培训。这类培训往往是专门应对某一项任务而产生，比如遇到部队要更换新的网络安全防御系统，就会有关于如何更换和操作新系统的

相关培训。这类培训并不固定，针对性和时效性较强。

三、存在问题

（一）培训体系整体上缺少官方统一的定义和标准

网络战需要什么样的能力？网络部队究竟需要什么样的培训来满足这些能力？这些问题在美军尚在讨论之中，因而目前官方还没有一个关于网络部队人员能力培养的明确、统一的定义和标准。由于美国网络司令部建立时间较短，目前相关条令体系还不完善，人员培训方面并没有制定出统一的条令和指令性文件。各个单位的网络相关术语也存在分歧。例如，术语“网络空间行动”和“计算机网络行动”究竟所指相同还是有所区别，使用上较为混乱。定义不清会导致培训出现一些混乱、重叠的现象。一些界定不明的培训内容会出现多个领域重叠。比如，网络战与情报工作在某些内容上有重叠，究竟由哪方负责培训没有明确的规定，而双方对于相同的内容重复培训就会造成浪费。其次，如果培训标准不明确，那么培训内容则容易出现无序状态，难免与实际工作相脱节，或出现培训内容扎推现象，导致整体培训效率不高。

美国国防部于2013 年12 月发布的报告《网络空间人才战略》中提出，“要建立一套在整个国防部范围内统一的关于网络空间人才管理的出版物”[11]，即关于建立一支合格的网络空间人才大军的一系列政策和指令文件。其中，具体提到要制定一套标准的网络空间工作职能的词汇表，建立网络空间工作岗位描述标准等，旨在解决这一问题。但截至本文完稿，未见相关出版物发布。

（二）培训内容重技术轻文化

当前美军网络部队的培训内容绝大多数都是关于网络应用技术的，辅以网络政策和战略方面的培训（供领导层）。而有人士指出，网络部队培训不应只局限于传统的“计算机天才的技能”，还应当包括外国语言和文化的培训[12]。因为网络战不仅停留在技术层面，在某些情况下，网络战士不能只懂计算机，还需要对对象国文化差异、风俗、国民性格、劝说策略等有深入了解，并且只有能读懂该国网站内容，才能更加有效的开展网络战。而语言与文化培训是当前美军网络部队培训所欠缺的，归根结底依然在于官方没有制定出明确、科学的培训标准。缺少对网络部队能力需求的详细、科学、全面的界定，相关培训也自然难以做到全面，往往只集中在大多数人认为最困难的技术层面的培训。

（三）一些培训欠缺选拔机制

网络技术培训耗时耗力，培训成本很高，如果受训人员不能达到某项培训的入门条件，则会更加费时低效。美军虽然已初步形成较为完备的岗位认证体系，但是选拔体制（特别是中高级培训）还停留在各组织单位自行决定和探索的阶段，远未形成一套成熟的体系。目前存在较多的现象是，一些需要一定门槛的培训项目因为没有正规的“筛选”机制，其培训对象存在较多的零基础人员，造成培训花费高、效率低。缺少科学的选拔机制，就难以实现把合适的人放到合适的培训机构。美国兰德公司研究员曾提议模仿“国防语言分级测试”建立一个网络技能测试评估体系，作为全军通用的选拔方法，但美军一些专业人士指出，网络技能的评估与外语能力的评估差别很大，前者更加复杂且内容更新换代很快[13]。有些网络技能难以通过考试来评估，只能通过观察其工作表现。有些高级培训的选拔方法采用百分比录取，例如从中级培训班中选出表现最好的前 8% 的培训学员接受高级培训。

总的来说，近些年美国网络部队的培训发展速度很快，已形成一套针对不同层次和不同任务、方式多样、规模庞大的培训体系，能够充分利用地方院校、私人企业等社会资源，基本上能满足当前美军网络部队工作的需要。但是由于在上层统一协调和条令制定上面进展较为滞后，造成整个培训体系存在一定程度的混乱、重叠、片面的问题。最后需要说明的是，出于敏感性，美国军队和政府正式出台的相关文件和公开发表的论文几乎很少涉及网络进攻领域的培训，大都集中在网络防御方面，这就造成了本文的分析存在一定的局限。

参考文献：

[1] U. S. Department of Defense. Cyber Operations Personnel Report: Report to Congressional Defense Committees [R]. Washington, D. C.: Government Printing Office, 2011: 4 - 5.

（下转第 120 页）