

美军网络空间作战指挥控制发展研究

王炜¹, 郭宏生², 韩笑¹

(1. 95899 部队, 北京, 100085; 2. 91772 部队, 北京, 102206)

摘要: 网络空间作战的指挥与控制关系是组织实施网络空间军事行动的关键。美军一直在调整与改革网络空间这一新兴作战领域的作战指控关系。阐述了美军现行的指控关系, 研究归纳了美军网络空间作战指控发展的三个阶段: 以区域指控为中心、全球与区域指控并重、以全球指控为中心, 最后对美军网络空间作战指控的发展方向进行了研究。对指导我网络空间作战指控发展具有一定的参考价值。

关键词: 网络空间作战, 指挥控制, 指控关系, 指控链

0. 引言

近年来, 网络空间已被广泛认同是军事斗争的一个现实领域。美军为谋求网络空间的绝对优势, 抢占军事战略的制高点, 已正式将网络空间作为与陆、海、空、天并列的第五大军事作战领域^[1]。与此同时, 美军还积极推进网络空间力量的整合工作。2010 年, 美军成立美国网络司令部 (USCYBERCOM)^[2], 旨在梳理网络空间的指挥与控制 (Command and Control, C2) 关系, 集中行使网络空间力量的指控权。

然而一直以来, 美军都是按地理位置来划分战场责任域 (AOR), 地理作战司令官 (Geographic Combatant Commander, GCC) 在责任域内具有绝对的指挥控制权。网络空间的无界性、迅捷性和广泛性等特征显著区别于传统陆、海、空、天等物理域属性, 其指控模式势必对美军传统指控关系带来挑战, 造成 GCC 无法实现统一及同步的指控^[3]。

针对这些问题, 美军主要从两方面着手解决: 一是理顺网络空间作战 (Cyberspace Operations) 相关部门间的指控关系。通过出台法律法规及条例, 美军重点从顶层明晰多部门间的指控链, 包括明确战略司令部 (USSTRATCOM) 与网络司令部在网络空间的职权划分、网络司令部与各 GCC 在网络空间作战的指控关系、以及网络司令部与各军种网络作战力量间的指控关系; 二是加强网络空间作战指挥控制的研究。美军各作战司令部、各军种相继提出与自己实际情况相符的方案计划, 并进行了大量的实验和相关概念的技术演示验证。同时, 美军还持续资助军事院校、智囊组织等研究机构开展网络空间作战指挥控制学术研究, 丰富了美军网络空间的作战思想和理论。

1. 美军现行的指控关系

美国于 1986 年颁布的《戈德华特—尼克尔斯法案》(又称《国防部改组法》) 是对现行美军指控关系影响意义最大的法案, 该法案调整了美军在二战后实行的各军种独立指挥链模式, 正式确定了总统、国防部长到作战司令官的作战指挥链, 从而奠定了美军“军令”、“军政”分离的指控模式。

根据美军联合条令 (JP) 的定义^[4], 美军现行的指控链主要通过“军令”、“军政”两条主线来实施。其中, “军令”解决作战力量“使用权”问题, 主要包括作战指挥 (Combatant Command, COCOM)、作战控制 (Operational Control, OPCON)、战术控制 (Tactical Control, TACON), 分别从战略、战役、战术层面施行作战指控。“军政”解决作战力量“所有权”问题, 主要指行政控制 (Administrative Control, ADCON)。

图 1 为美军指控关系的简化模型图^[4]。由图可见, 美军的指控链通过总统与国防部长, 向下贯穿各级作战司令官 (CCDR)。其中, COCOM 一般由总统或国防部长赋予统一作战司令部 (UCC) 司令官, 即 GCC 与职能作战司令官 (Functional Combatant Commander, FCC); OPCON 可由各级作战司令官行使, 其主要职能包括组织和部署作战力量、制定作战目标、分配作战任务等; TACON 一般由低级别的作战部队行使, 其职能主要包括对完成指定的使命或任务进行细致的指导和控制。美军的 ADCON 一般由各军种行使, 其主要职能包括部队编制、装备人员训练、后勤保障、人事管理等。

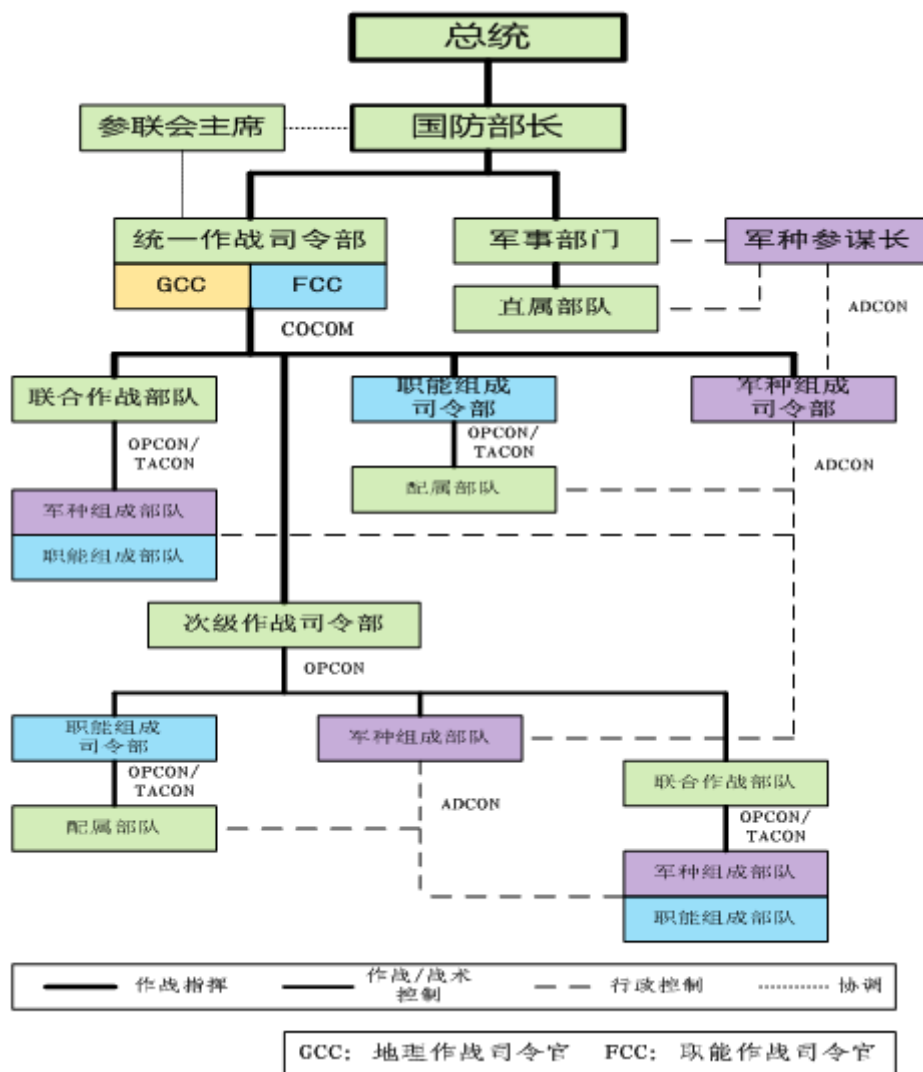


图1 美军C2简化模型图

美军认为指挥控制是所有军事行动的核心，其各级作战司令部的指挥控制体系历经多年考验，已臻完善。但随着网络空间概念的兴起，各级相关作战力量的组建，特别是2008年《统一指挥计划》(UCP)^[5]的颁布，在一定程度上影响了美军现行的指控关系。近年来，美军对网络空间指控关系的讨论一直没有停息过，而其争论的焦点就是各部门在网络空间作战中应该履行什么样的角色。

2. 美军网络空间作战的指控关系演进

与美军其它作战领域类似，美军在网络空间作战的指控关系一直在调整与改革。归纳起来，美军网络空间作战的指控关系经历了以下三个阶段：以区域网络作战指挥为中心、全球网络作战指挥与区域网络作战指挥兼顾、以全球网络作战指挥为中心。

2.1 阶段一：以区域网络作战指挥为中心

美军早期的网络作战（Network Operations, NETOPS）与其它领域作战一样，采用“作战司令部—作战部队”的组织架构。1998年，美军认为这种作战模式已不适合网络空间作战的指挥控制，需要建立一个集中控制的网络作战部门。为此，美军最早由国防信息系统局（DISA）组建了计算机网络防御联合特遣部队（JTF-CND），后又相继改组为计算机网络作战联合特遣部队（JTF-CND）、全球网络作战联合特遣部队（Joint Task Force-Global Network Operations, JTF-GNO），并移交给美战略司令部指挥^[6,7]。

图2为早期美军网络作战指控关系的简化模型图。在此阶段，JTF-GNO并没有对各战区网络作战部队

的指控权，网络作战的 **OPCON** 及 **TACON** 分别由各 GCC 的战区网络作战控制中心（Theater Network Operations Control Center, TNCC）及战区网络作战中心（Theater Network Operations Center, TNC）来负责，JTF-GNO 的主要职能是协调与支援。这种指控模式过于强调 GCC 对其负责区域的指挥控制，被美军证明不利于网络空间态势感知及全球性网络作战的指控^[6]。

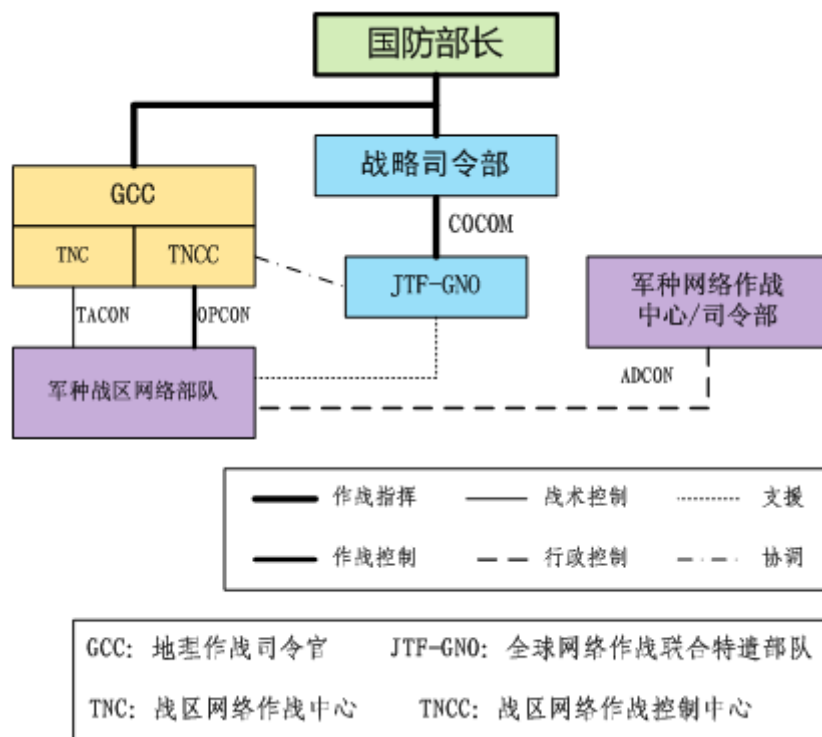


图2 早期美军 NETOPS C2 简化模型图

2.2 阶段二：全球网络作战与区域网络作战指挥兼顾

2005 年美军提出 GIG 网络作战的联合作战概念（CONOPS）^[8]，进一步加强了战略司令部及 JTF-GNO 的网络作战职能。根据作战概念，美军将网络作战划分为两种模式：全球性网络作战、战区性网络作战，并根据网络作战造成的实际影响决定采用何种网络作战指控模式。

图 3 为美军全球网络作战指控关系简化模型图^[6,8]。在全球网络作战模式中，战略司令部是受援对象，接收其它 FCC、GCC、以及军种力量的支援。战略司令部方面，JTF-GNO 通过全球网络作战中心（Global Network Operations Center, GNC），对全球网络作战支持中心（GNSC）、GIG 框架服务管理中心（GISMC）、全球卫星通信支持中心（GSSC）等职能网络作战部队，以及各 TNC、各军种网络作战组成部队实施 **OPCON**。其它 FCC 方面，通过全球网络作战控制中心（GNCC）对其隶属网络作战部队实施 **OPCON**，并与 JTF-GNO 保持协调关系。GCC 方面，通过 TNCC 对其隶属网络作战部队实施 **OPCON**，与 JTF-GNO 保持协调关系，并接受 TNC 的支援。军种方面，军种网络作战组成部队主要以网络作战与安全中心（NOSC）、计算机应急响应小组（CERT）、计算机事故响应小组（CIRT）等形式存在，并在必要时能够接受 JTF-GNO 的直接 **TACON**。

图 4 为美军战区网络作战指控关系简化模型图^[6,8]。在战区网络作战模式中，GCC 成为受援对象，接受战略司令部、其它 FCC、以及军种力量的支援。战略司令部方面，JTF-GNO 在保留对 GNSC、GISMC、GSSC、各军种网络作战组成部队 **OPCON** 的同时，将对 TNC 的 **OPCON** 转变为支援关系。其它 FCC 方面，GNCC 不再与 JTF-GNO 保持协调关系，而是直接与 TNCC 保持协调关系。GCC 方面，TNCC 与 TNC 指控关系由支援转变为直接的 **OPCON**。与全球模式相比，战区模式下增强了各 GCC 对其辖区内网络作战的指控。

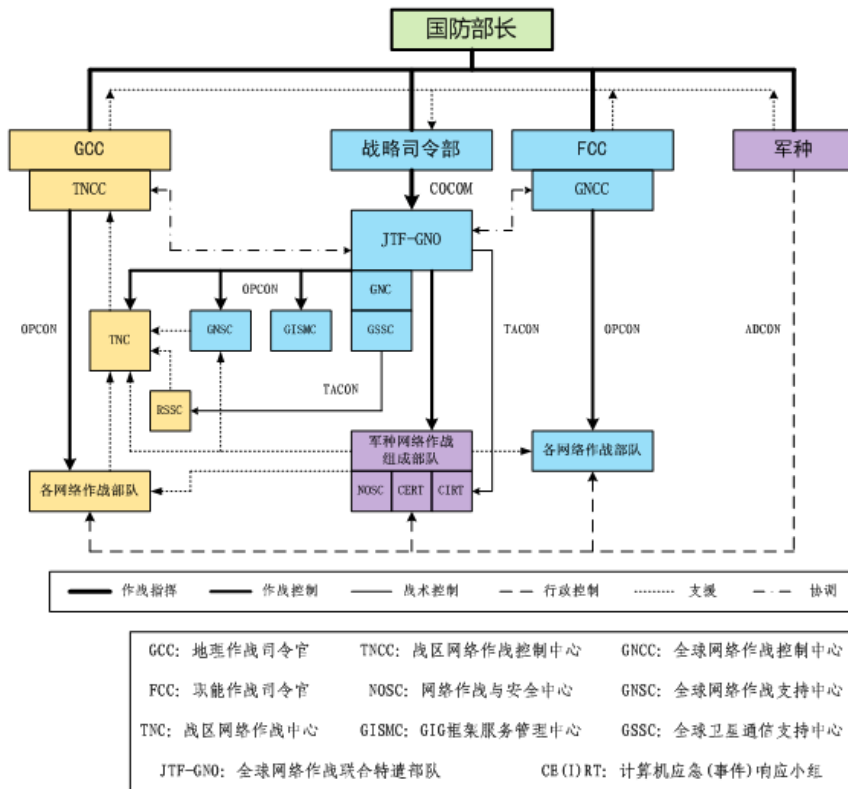


图3 全球 NETOPS C2 简化模型图

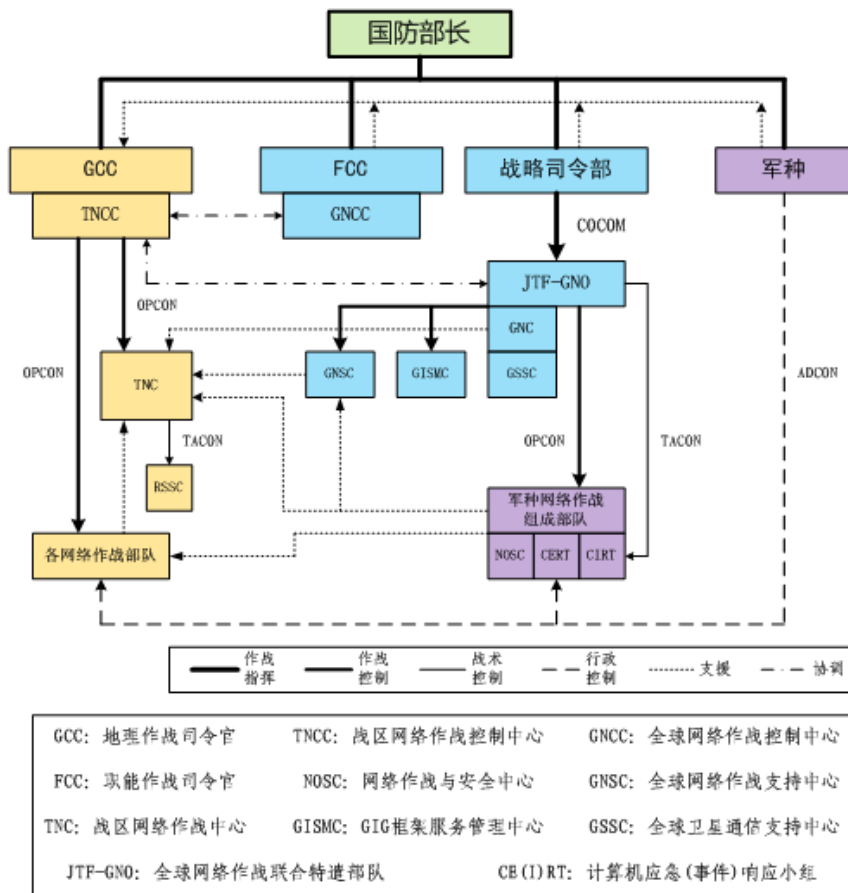


图4 战区 NETOPS C2 简化模型图

相比阶段一的指控关系,阶段二的指控结构更加适用于网络作战多样性特征,使得美战略司令部、GCC、FCC、以及军种网络作战力量的整体角色都得到了加强。

2.3 阶段三:以全球网络空间作战指挥为中心

2010年10月,美网络司令部正式具备全面作战能力(FOC),标志着美军对网络空间作战的认识进一步深化,体现在指控关系上主要有两个方面^[9,10,11,12]:

一是加强网络空间作战全球统一指挥。随着网络空间在国家战略及军事战略地位作用的提升,美军在作战概念上逐渐将网络作战向网络空间作战演化,更加强调网络空间的广泛脆弱性、网络事件的无界及瞬间性、网络作战行动的快速性等。因此,根据2011年的《统一指挥计划》^[13],美军进一步加强了网络空间作战的全局指控,除美战略司令部仍保留网络空间作战的COCOM外,美网络司令部在网络空间作战上有绝对的控制权;

二是加强网络空间防御与攻击作战的统一指挥。美网络司令部是由JTF-GNO与网络战联合职能司令部(JFCC-NW)合并而成。根据美国法典(USC),前者属于法典第10篇(Title 10)^[14],主要注重网络空间防御作战行动;后者属于法典第50篇(Title 50)^[15],主要注重网络空间攻击作战行动。通过成立网络司令部,美军有效的整合了网络空间防御与攻击作战力量。

图5为现阶段网络空间作战指控关系简化模型图。现阶段的网络空间作战指控不再区分全球与战区模式,美网络司令部在攻防两端均具有网络空间作战的集中控制权,具备美法典Title 10与Title 50的双重关系(DUAL-HAT)。Title 10方面,军种组成部队包括空军第24航空队、陆军网络司令部、海军舰队网络司令部、海军陆战队网络司令部等军种网络司令部;网络司令部对各军种网络司令部实施OPCON,军种网络司令部通过各作战中心(OC)对部署在各战区的军种网络作战组成部队实施OPCON,各军种网络作战组成部队通过NOSC对战区内各网络作战部队实施TACON;同时,为了满足各GCC的作战需求,网络司令部通过在各GCC嵌入网络支援单元来协调网络空间作战与传统作战领域其他作战行动的关系。Title 50方面,军种组成部队包括空军情报侦察监视局、海军网络战司令部、陆军情报与安全局、海军陆战队情报局等;网络司令部通过国家安全局,对各军种组成部队实施支援。

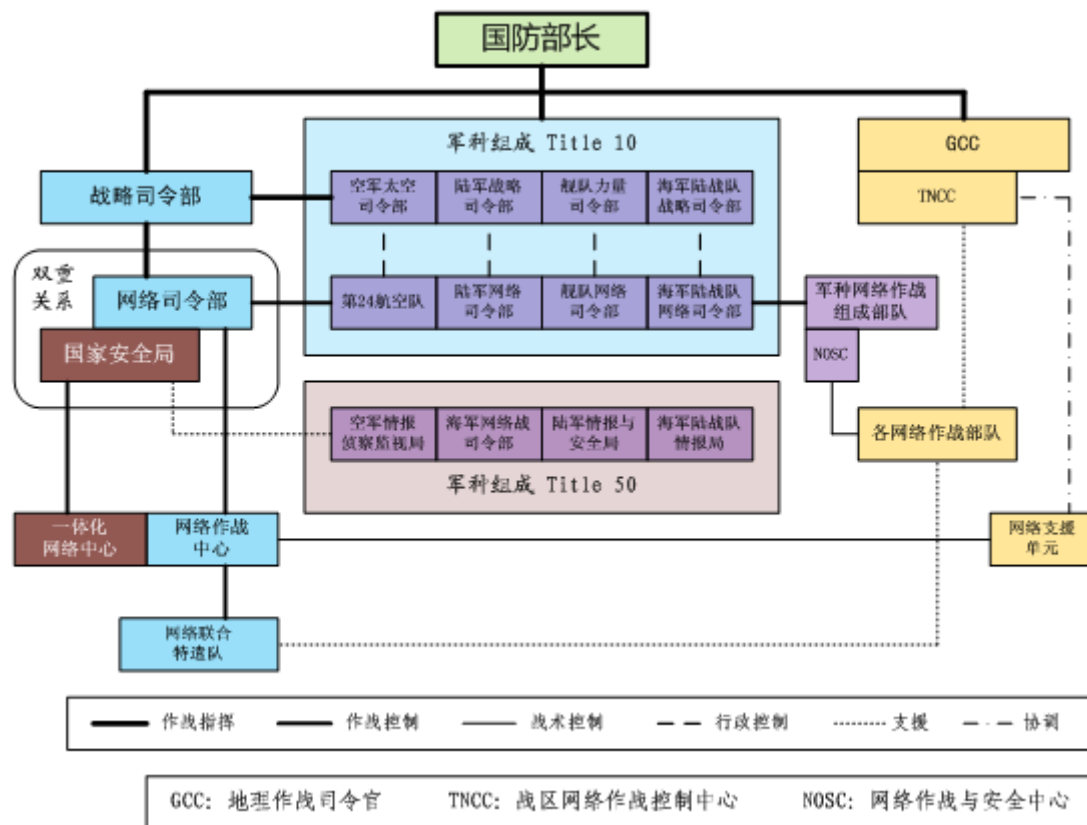


图5 现阶段网络空间作战C2简化模型图

3. 美军网络空间作战指控关系的发展方向

2012年, 美军联合条令 JP 3-12《网络空间作战》^[16]未被批准实施, 表明美军对网络空间作战的相关问题尚未考虑成熟, 美军在不断探索网络空间作战内涵与外延的同时, 大力开展网络空间作战的军事理论与实践, 从法律、政策、体制、编制等多个层面梳理网络空间作战的指挥控制关系。从近年来美军在网络空间的举措和研究来看, 未来美军网络空间的指控关系可能有以下几个调整方向^[17,18,19,20,21,22,23,24]:

一、升格网络司令部。根据《联合指挥计划》, 网络司令部目前是隶属于战略司令部的次级职能司令部, 在实施网络空间作战的绝对控制权方面有一定的法律限制。下一步, 美可能在法典 Title 10 的框架下, 将美网络司令部升格为统一作战司令部, 由美总统与国防部长直接赋予网络空间作战的 **COCOM**, 从而实现网络空间作战的统一指控。

二、在 GCC 组建专门部队。目前, 美网络司令部是通过各军种网络空间作战力量, 对部署在各战区的网络空间作战力量实施间接的 **OPCON**。下一步, 网络司令部可能会效仿其它 FCC (如特种作战司令部) 的做法, 在各 GCC 成立战区网络中心 (Theater Cyber Center, TCC) 或联合部队网络功能组成司令部 (Joint Force Cyber Functional Component Command), 从而实现对各战区网络空间作战力量的直接指控, 形成一个更加简单、明确的指挥链。

三、细分网络空间防御与进攻的指挥链。美军现行攻防一体的网络空间作战指挥体制仍存有争议。主要原因在于, 网络空间防御作战本质上需要一个长期、统一的努力, 而网络空间进攻作战通常是瞄准特定的作战范围, 时间非常短暂, 并且每次作战情况都截然不同。下一步, 美军可能在加强网络空间防御作战全球统一指控的同时, 赋予 GCC 更多网络空间攻击作战的指控权限。

4. 结束语

如何理顺网络空间作战的指控关系, 是组织实施网络空间作战军事行动首先要解决的问题。美军认为, 为了有效地研究网络空间作战的指控关系, 首先需要确定“谁指挥”的问题, 并在此基础上, 逐步解决“网络空间作战在哪里发生, 有多少个部门参与到网络空间作战中, 各自履行的职责是什么”等诸多问题。为此, 美军通过确立网络空间作战的最高指挥机构, 自上而下的形成与完善其网络空间作战指控链。

虽然我军在体制结构上与美军有很大的不同, 但美军网络空间作战指控关系的演变思路, 以及其在政策法规、力量构成、体系能力等方面的经验做法, 都值得我们深入的学习与研究。

参考文献:

- [1] Robert M. Gates, Quadrennial Defense Review, 2010
- [2] DoD Fact Sheet on U.S. Cyber Command, 2010
- [3] Stephen M. Rodriguez, USCYBERCOM: A Centralized Command of Cyberspace, 2011
- [4] US Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, Joint Publication 1, 2009
- [5] US Department of Defense, Unified Command Plan, 2008
- [6] Peter J. Beim, Network Operations: The Role of the Geographic Combatant Commands, 2007
- [7] Robert A. Barker, Command and Control of Network Operation, Army War College, 2009
- [8] US Strategic Command, Joint Concept of Operations for Global Information Grid NetOps, 2005
- [9] Keith B. Alexander, U.S. Cybersecurity Policy and the Role of U.S. Cybercom, Speech at CSIS Cybersecurity Policy Debate Series, 2010
- [10] Keith B. Alexander, Building a New Command in Cyberspace, Strategic Studies Quarterly, 2011
- [11] Keith B. Alexander, Posture Statement to the House Armed Services Subcommittee on Emerging Threats and Capabilities, 2011
- [12] Keith B. Alexander, Statement before the Senate Committee on Armed Services, 2012
- [13] US Department of Defense, Unified Command Plan, 2011

- [14] United States Code, Title 10, Armed Forces
- [15] United States Code, Title 50, War and National Defense
- [16] US Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12, First Draft, 2011
- [17] Joseph H. Scherrer, William C. Grund, A Cyberspace Command and Control Model, Air University Press, 2009
- [18] David M. Hollis, USCYBERCOM: The Need for a Combatant Command versus a Subunified Command, 2010
- [19] David M. Hollis, Cyber Defense: U.S. Cybersecurity Must Do's, Armed Forces Journal, 2011
- [20] Tamara M. Keene, Organize and Optimize: CYBERCOM's Need to be a Unified Command, 2011
- [21] Harry M. Friberg, U.S. Cyber Command Support to Geographic Combatant Commands, Army War College, 2011
- [22] Jeffrey A. May, A Model for Command and Control of Cyberspace, Army War College, 2012
- [23] Daniel C. Wood, USCYBERCOM: Right Solution, Wrong C2 Structure, Naval War College, 2012
- [24] Andrew Feickert, The Unified Command Plan and Combatant Commands: Background and Issues for Congress, 2013