网络战支持的工作说明书

非官方中文译本 • 安天技术公益翻译组 译注

文档信息			
原文名称	STATEMENT OF WORK FOR CYBER WARFARE SUPPORT		
原文作者	HBGary 公司	**原文发布日期**	2009 年 10 月 30 日
作者简介	HBGary 是 ManTech International 的子公司 ,专注于技术安全。在过去，两个独立但关联的企业采用了 HBGary 名称：即 HBGary Federal （向美国联邦政府销售产品）和 HBGary, Inc。它的客户包括信息安全公司、计算机应急响应团队和计算机取证调查团队。2012 年 2 月 29 日 ,HBGary 公司宣布被 IT 服务公司 ManTech International 收购。与此同时，HBGary Federal 已上报关闭。 http://en.wikipedia.org/wiki/HBGary_Federal		
原文发布单位	HBGary 公司		
原文出处	http://info.publicintelligence.net/HBGary-CyberWarfare.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学		

	习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

网络战支持的工作说明书

2009 年 10 月 30 日

1.1 简介

1.2 背景

网络战是网络空间领域的战争，SECDEF 将网络空间定义为“信息环境的全球性领域，由信息技术基础设施的相互依存的网络组成，包括互联网、电信网、计算机系统，嵌入式处理器和控制器。”网络战包括计算机网络作战（如攻击、防御和开发）、信息安全保障以及网络作战（包括网络空间内发生的命令、控制、通信、情报、监视和侦察（C4ISR）、信息战（IO））。这包括针对自动化系统（如 C4ISR）的计算机网络作战，以及定义人机交互的物理、社会和生物网络之间的相互作用。太平洋空间和海战系统中心（SSC PAC）是 C4ISR 系统和 IO 的海军研究、发展、测试和评估（RDT＆E）和信息获取中心，其职责包括：任务分析、技术基地的评估和发展、基础研究、技术示范、支持生产、支持作战部队、支持政策和战略制定以及网络战方面的众多国家和战术系统的整合。

SSC PAC、美国国防部和其他政府客户越来越多得寻求咨询、援助、协调和必要的产品（支持作战规划、评估、整合和技术开发，保证作战人员在网络空间领域占据优势）。实现网络空间优势的具体活动包括，但不限于：

- 计算机网络作战（如攻击、防御和开发），因为它们涉及信息技术基础设施相互依存的网络，包括互联网、电信网、计算机系统、嵌入式处理器和控制器。
- 针对自动化系统的计算机网络攻击（CNA）和计算机网络开发（CNE），以及定义人机交互的物理、社会和生物网络之间的相互作用。
- 信息保障（IA）和计算机网络防御（CND）措施来保护和捍卫海军、联合和国家系统。
- 网络战任务保证和任务规划。
- 了解人类行为和认知功能来影响对手决策制定（如心理战（PSYOP）和军事欺骗

（MILDEC）。

- 电子战（EW），包括射频、毫米波和光环境中的电子攻击（EA）、电子支援（ES）和电子保护（EP）。

- 监控、分析和减轻作战安全（OPSEC）漏洞。

- 网络战能力的命令和控制（C2） 。

- 网络战方面（包括空间战）的情报、监视和侦察（ISR）。

- 无处不在的通信和计算环境。

- 对策，包括开发源识别工具、网络数据管理、对象关联和引用方法的能力和知识。

- 未来环境的建模、仿真和可视化，其中通信、计算、数据、传感器和网络是互操作的、无处不在的、透明的。

- 了解网络是一门科学，开发模型（可以清晰的显示网络如何运作、如何抵制或阻止攻击）。

- 物理、生物和社会网络的融合以及这将如何影响人类互动和决策周期。

- 了解网络战的理论、战术、技术和程序（TTP）。

本合同项下的条款将支持 SSC PAC 开发能力和提供技术服务，以支撑海军、国防部和其他政府机构在网络空间的技术和作战活动。

1.3 范围

本合同的范围包括从战术、作战和战略层面研究网络战系统的架构、工程学、功能、接口和互操作性，服务和功能。这包括作战演习设计和实施、运营和需求分析、概念形成和发展、可行性演示和作战支持。这将包括分析和工程化作战、功能和系统要求，以建立国家、战区和军队层面的架构和工程计划，接口，系统规范和定义，以及实施；包括监测系统的硬件购置。其他行动包括软件设计和实现，以及系统集成、测试、评估和演示。

先进技术及特殊技术作战的研究和发展要求技术或科学性的定期提高，以满足技术和作战目标及/或要求。也需要承包商的支持来补充或提供具备具体专业知识的人才，而 SSC PAC 的专业知识是有限或缺乏的。所需的专业知识领域可能包括，但不限于：网络战理论/战术、

技术和程序（TTP），政策和战略，作战计划分析，情报评估，有效性措施（MOE）和绩效措施（MOP）评估，电子战，军事演习，建模与仿真，系统工程，系统分析，计算机硬件/软件工程和开发，实施和集成，作战研究和分析，通信，网络硬件，协议和安全。

以下内容是目前存在或 2020 财年预期产生的合理的需求类型。因为需求任务的多样性，具体工作会以交付/任务订单的方式启动，交付/任务订单按照本工作说明书（SOW）的规定和其他协议条款发布。

- 对网络战、应用技术、技术和理论进行基础和应用研究。
- 设计和开发能够支持新技术和能力快速发展和实现的网络、系统、服务和应用架构；这些技术和能力反映了快速发展的网络攻击技术。
- 分析、设计、开发、记录、集成、测试、安装和维护网络战和支持能力。
- 开发、实施和集成解决方案，形成整体的命令与控制能力，配合适当的支柱技术和能力，支持机构间交流和网络活动合作。
- 将网络战系统、工具、技术和流程（包括现有的和新的）引入作战环境之前，提供它们互操作性的测试基地（通过 SSC PAC 实验室及其他政府设施）。
- 参与网络技术论坛。
- 提供作战支持，以协助网络战、可行系统、程序和功能的技术和方案监督。
- 提供系统工程和集成支持，以提高网络战和可行系统、服务和功能的整体有效性。
- 演示和评估网络战、可行系统和功能的先进软件和硬件理念和技术应用。
- 搜索发布在网络空间的物理身份和初始位置信息。
- 执行分析和系统工程，以开发能够支持新兴网络战要求的措施。
- 开发能力，以检测并识别对手的复杂多维攻击，并能够将离散事件与其对作战人员的影响联系起来。
- 提供计算机和网络取证能力。
- 进行分析、算法开发和实施，并展示来自各种渠道的网络战工具和数据。
- 支持网络战的实验、演习和其他活动。

- 分析对抗网络威胁的能力，以开发各种假想情境下的行动和应对方案。
- 开展网络战建模与仿真，军事演习和分析。
- 执行风险评估和缓解规划。

1.4 参考文件

本 SOW 的编写参考了下列文件：

a. 网络空间政策回顾，2009 年 5 月
b. 信息战联合条例，Joint Pub 3-13，1998 年 10 月 9 日，非机密
c. 中央情报指令 7/3 信息战和情报界相关活动（U）
d. 海军网络作战概念，2009 年 6 月 2 日（草案）
e. 国家安全战略，2006 年 3 月
f. 国家军事战略--网络作战（NMS -CO）， 2006 年 12 月
g. 保护网络空间的国家战略（国家安全总统指令 38（NSPD - 38））, 2004 年
h. 海军作战 Pub 3-63 CNO 第 1 卷和第 2 卷
i. NTTP 3.13.x 系列海军信息战
j. 网络安全和监控（国家安全总统指令 54（NSPD-54）/国土安全总统指令 23（HSPD-23））, 2008 年 1 月 8 日
k. DODD O- 8530.1 （CND）
l. DODI O- 8530.2 （CND）
m. CJCSM 6510.01 （DID：CND）
n. SECNAVINST 5239.19 （DON 事件响应/报告）
o. SECNAVINST 5000.2C，国防采集系统和联合能力集成与开发系统的实施和运作
p. 美国海军海洋系统司令部指令 3900.8A ,人类系统集成（HSI）的采集和现代化政策 ,2005 年 5 月 20 日

2.0 技术要求

承包商需要具备全方位网络战和可行活动的专业知识。

2.1 总则

承包商应提供技术和管理服务，以支持 SSC PAC 建立和维护网络战、可行产品线、计划和项目。承包商应提供有经验的人员从事鉴定和开发核心技术和功能服务，从而支持全方位的网络战。承包商应提供技术和管理服务，支持新能力的快速开发和部署，从而根据需求攻

击、防御以及开发网络、系统和服务。

2.2 技术评估、发展与转型

承包商应确定行业、学术界和乞讨者政府机构的技术，并对其进行研究、分析、替代方案分析（AoA）、评估、开发和测试，包括商业现货（COTS）、政府现货（GOTS）和开源技术，以便解决网络战的不足、改进现有的网络战、启用功能和/或开发新的网络战能力。

为了及时解决网络安全缺陷，承包商应建立核心技术的评价标准、指标、数据库和测试协议，并建立技术库，以便自动评估用于网络基础设施的新兴技术。拥有公共数据库（代表实际数据）的非机密实验室应使促进适当的系统工程分析和共同标准，以便进行比较、概念细化以及选择更先进的分析和研究。

2.3 需求分析

承包商应在军队、战区、作战司令部（COCOM）和国家层面执行现有及新兴业务和功能需求的分析，从而支持理论、战略、计划、经营理念、战术、技术和程序的开发和评估，以便向作战人员提供全频谱的网络战和作战能力。这应包括网络战机构的分析，包括用于开发新理论、作战方法和任务、潜在威胁的识别、漏洞、风险、安全保障、性能信标及对策的战术、技术和程序。承包商应分析潜在对手的社会和文化因素，以及相应的认知、行为、技能和知识要求。承包商也应分析系统或作战概念的可行性，包括成本/效益分析。承包商应研究并形成技术分析和评估报告（包括网络要求、能力和培训）。承包商应研究符合能力要求的海军、战区以及联合计划和方案，并形成报告、文件和评估报告。承包商应执行网络军事效用评估（MUA）/作战效用评估（OUA），包括网络作战能力评估和新兴技术的效用评估。

2.4 系统工程

承包商应在系统、内/间节点、军队、战区和国家层面进行系统的分析、架构、工程和集成服务。承包商应分析目前网络战及其能力和不足，确定系统要求和相关架构，并执行全方位的系统工程支持，以便实现全频谱的网络战能力和系统。承包商应进行技术贸易研究，从而指导新型网络战架构和详细工程设计的开发。

2.5 作战和技术支持

承包商应审查和分析国家安全政策和军事战略、包括国防转型和规划引导、情报预测、威胁预测、脆弱性评估、取证和其他有关材料和活动，从而向 SSC PAC 网络战提供作战和技术支持。承包商应支持全面、长期、全面集成的国防部策略的开发和实施，从而开发支持国家安全和战区作战计划的创新方法。结合之前的规划和战略开发结果，承包商应支持战区战略、作战概念、标准作战程序、交战规则、预计响应、以及作战指挥官/联合特遣部队（JTF）指挥官作战/应急计划（OPLAN / CONPLAN）的开发。此外，承包商应支持战区、国家和全球利益相关者之间形成谅解备忘录/协议备忘录（MOU/MOA）。

承包商应提供战区全方位的安全测试和评估活动，包括 Blue、Green、White 和 Red 团队的支持，从而提供培训、评估脆弱性和/或网络战能力的不足（针对来自敌人或其他恶意来源的最新威胁）、并确定解决方案和/或权衡方法。

承包商应参与要求的网络战论坛、会议、研讨会、演习和规划会议。

承包商应提供取证被入侵系统以及被捕获系统的取证支持。这种支持应包括分析软件、固件、硬件（模拟和数字部分）、保护措施（包括防篡改/证据系统）。

2.7 演习和实验支持

承包商应提出并参与练习和实验（包括战争演习），以支持网络战及其能力和工具的开发和评估，从而确定全频谱网络战的新战术、技术和程序。这应包括演习和实验的所有规划、物流、调度以及人员配备要求。其他要求包括但不限于：

a) 详细的演习和实验设计、规划和计划，包括设备、平台、系统（包括配置）的规范，演习代号/脚本和人员。

b) 制定模拟功能和/或网络战的功能作战的验证模型，及相应能力或活动。

c) 物流支持，包括配置管理、质量保证、可靠性/可维护性分析、材料/数据控制和分类/信息安全监督。

d) 参与演习和实验，包括学科专家（系统或活动观察员，或数据收集人员）。

e) 根据实际收集的信息分析和重建演习和实验数据。

f) 制定网络战训练目标，以刺激培训人员、评估能力不足并制定行动和里程碑计划。

g) 研究、收集、分析和开发情报；信息战概念开发；规划实验文件和实施。

2.8 软件开发和原型设计

承包商应指定、设计、开发、编码、测试、集成和记录软件模块、系统和子系统，以提供新的功能并改进现有网络战和系统。承包商应执行软件组件和系统的逆向工程，以支持脆弱性和开发分析。需要实现的功能包括全频谱的网络战。承包商应坚持开放标准和现代软件开发方法，包括业界认为“最好”的方法。这也包括满足严格时间要求的快速原型开发。

2.9 硬件开发和原型设计

承包商应向基于硬件的全频谱网络战和能力解决方案的开发、原型设计、实施、测试、集成和记录提供硬件工程支持。承包商应执行硬件组件和系统的逆向工程，以支持脆弱性和开发分析。这包括混合信号集成电路的设计与开发。承包商应坚持现代化的硬件开发和制造方法，包括业界认为“最好”的方法。这也包括满足严格时间要求的快速原型开发。

2.10 建模与仿真

承包商应构建、设计和开发的建模与仿真（M&S）基础设施和能力，以调查系统及其相互依存关系，加强网络战进攻和防御措施的防范、保护、响应、缓解和恢复活动。M&S 应针对网络应急分析、网络攻击分析、态势评估、行动纲领分析和优化。M&S 也支持多项业已存在的 M&S 的功能整合和新能力开发。

2.11 培训支持

承包商应策划、制定和实施网络战训练计划、教育和培训课程、正式网络演习（实施网络战攻击、防御、和开发能力）。

2.12 安全工程

承包商应执行美国国防部信息技术安全认证和认证过程（DITSCAP）/国防信息保障认证和认证过程（DIACAP）的各个阶段、所有安全测试和评估阶段，并提供全面的风险评估做

为个人交付/任务订单履行的一部分。承包商应根据 DITSCAP / DIACAP、秘密及以下互操作性（SABI）和中央情报指令（DCID）6/3 进程支持项目的认证。承包商也应对安全测试计划、程序、报告和评估进行分析。

3.0 报告、数据和成果

个人交付/任务订单指出，技术数据和计算机软件成果应当按照合同数据需求清单， DD 表单 1423 来提供。最终验收前，所有成果必需经过 SSC 委员会的审查和批准。

所有机密成果应受到保护，并按照标准的安全做法和程序办理。

4.0 安全

这项任务的性质需要访问机密信息。承包商的工作包括访问非机密和机密数据、信息和空间。承包商将被要求参加机密级别的会议。

所有的工作都要按照美国国防部和海军最终安全(OPSEC)的要求，以及 DD254 的 OPSEC 附件进行。