美国NICE网络空间安全人才队伍框架探析

韩 臻 王 星 黄学臻 吕从东

[1]北京交通大学国家保密学院 [2]北京交通大学计算机与信息技术学院

1 引言

2010年4月，美国启动“国家网络空间安全教育计划”（National Initiative of Cybersecurity Education，NICE），期望通过国家的整体布局和行动，在信息安全常识普及、正规学历教育、职业化培训和认证等三个方面开展系统化、规范化的强化工作，来全面提高美国的信息安全能力。2011年8月，美国国家标准技术研究院发布了《NICE战略计划（草案）》，并在网上公开征集意见[1, 2]。其中，一项重要的基础性工作是要为网络空间安全这一新兴领域定义一致通用的术语来描述专业范畴、职业路径，及其岗位能力和资格认证等。为此，NICE于2011年9月公布了《NICE网络空间安全人才队伍框架（草案）》（NICE Cybersecurity Workforce Framework），并在网上公开征求各方意见[3, 4]。该《框架》给出了网络空间安全工作的分类法及其通用词汇，并对每种职位的任务，以及所需的“知识、技能、能力(KSAs)”进行了详细的描述，这对开展网络空间安全专业学历教育、职业培训和专业化人才队伍建设有重要的影响和指导作用。

公布的《框架》由摘要[3]和详细完整版[4]两个文档组成，本文将简要介绍该《框架》的结构和主要内容，供读者了解和参考。

2《框架》的定位和结构

《框架》中首先指出：由于美国尚没有对网络空间安全工作有统一的定义，各部门在职业、职称和职位描述等方面存在很大差异，从而没有一个共同的语言来讨论和理解网络空间安全专业人员的工作和技能要求，这给国家制定信息安全技能基线、确定技能缺口和差距，以及人才队伍的培养造成了障碍。因此，迫切需要为网络空间安全工作及工作人员建立并使用一套通用的词汇、分类法及其他数据标准，这是关系到NICE计划成功与否的核心工作。制定《NICE网络空间安全人才队伍框架》的最终目的，就是要确保它能够成为美国创建和持续拥有一支世界一流的网络空间安全人才队伍的坚实基础。

《网络空间安全人才队伍框架》根据通用的词汇及分类法来定义网络空间安全工作和队伍。目前，该《框架》初稿主要由联邦政府（特别是情报部门和国防部）参与制订，但其目标是希望被整个美国采纳和使用，所以NICE呼吁美国全国的学术界、网络空间安全组织及私营企业等各个领域也共同参与来完善该《框架》。

《框架》用“群体”来概括定义网络空间安全人才队伍，根据工作所需的能力或职业发展路线，采用专业领域（Specialty Area）结构将网络空间安全工作职能和人员进行分组。目前，《框

架》草案将网络空间安全专业领域划分为七个大类，包括：安全地提供（Securely Provision），运营与维护（Operate and Maintain），保护与防御（Protect and Defend），调查（Investigate），作战与搜集（Operate and Collect），分析（Analyze），支持（Support）。其覆盖的主要工作职责与信息技术、信息保障和计算机科学等相近技术领域相关。除了那些能够使网络空间安全专业人员高效地完成其工作的关键支持（Support）角色外，有关采购、物理安全、关键基础设施监管、电气工程等职业专长没有包括在内。所以，该《框架》的意图及其提供的职业发展计划是为了更好地理解如何培训和配备具有计算机网络（cyber）技能的工作队伍。

《框架》中详细给出了每个专业领域对应的典型任务（Task）和应具备的知识、技能和能力（KSAs），以及各个专业领域的职位举例。当然，职位名称并不是关键，重要的是明确特定专业领域的定义、任务及其KSAs。《框架》中对所有的Task和KSA进行了编号，共列出了432项不同的Task，296项不同的KSA，但有两个特殊专业领域未给出相应的Task和KSAs。其中，一些Task或KSA会在不同的专业中同时出现，体现了部分工作的些许重叠和部分KSAs的共性需求。

完整版的《框架》草案原版英文文档是由页面化结构组成的PDF文档[4]，阅读和信息查找非常方便。点击首页上代表七个类别的方框或页面底部的按钮，可以导航到对应类别的页面。在点击进入某个类别之后，可以继续点击选择各专业领域，查看其详细视图——以表格方式展示的Task和KSAs，并可以随时切换。另外，文档还提供了搜索功能。

3《框架》的七大类专业领域

3.1 安全地提供

该大类专业领域涉及构思、设计和建设安全IT系统，负责系统开发的某些方面，包括七种典型专业岗位。

（1）信息保障合规性（Information Assurance Compliance）：专业人员负责对文档编撰、系统验证和鉴定等过程进行监督和评估并提供支持，以确保新的IT系统能够满足组织的信息保障（IA）需求，保证系统对内和对外保持合规性。《框架》列出了该岗位的13项具体任务，以及需要具备的11项KSAs。

（2）软件工程（Software Engineering）：专业人员负责开发、创建及编写/编码（或修改）计算机应用程序、软件或专门的实用程序。《框架》列出了该专业的28项具体任务以及需要具备的34项KSAs。

（3）企业架构（Enterprise Architecture）：专业人员负责开发系统的概念，工作于系统开发生命周期的能力定义阶段，将技术和环境条件（例如法律和法规）转化为系统和安全设计及其开发过程中的具体要求。《框架》列出了该专业的21项具体任务，以及需要具备的44项KSAs。

（4）技术论证（Technology Demonstration）：专业人员负责实施技术评估和集成过程，提供和支持原型样机的能力并评估其功效。《框架》列出了该岗位的7项具体任务，以及需要具备的5项KSAs。

（5）系统需求规划（Systems Requirements Planning）：专业人员负责与客户协商以收集和评估客户的功能需求，并将这些需求转化为技术解决方案。负责向客户提供信息系统适用性的指导，以更好地满足业务需要。《框架》列出了该专业的16项具体任务，以及需要具备的39项KSAs。

（6）测试与评估（Test and Evaluation）：专业人员负责开发和实施系统测试，以期通过采用成本效益的原则和方法，规划、评估、检验和验证系统或者包含信息技术的系统要素的技术、功能和性能特征对详细设计书和需求的符合程度。《框架》列出了该专业的10项具体任务，以及需要具备的16项KSAs。

（7）系统开发（Systems Development）：专业人员主要工作于系统生命周期的开发阶段。《框架》列出了该专业的47项具体任务，以及需要具备的49项KSAs。

3.2 运营与维护

该大类专业领域负责提供必要的支持、管理和维护，以确保切实有效的IT系统性能和安全性，包括七种典型专业岗位。

（1）数据管理（Data Administration）：专业人员负责开发和管理数据库和（或）数据管理系统以允许数据的存储、查询和使用。《框架》列出了该专业的15项具体任务，以及需要具备的23项KSAs。

（2）信息系统安全管理（Information System Security Management）：专业人员负责监督信息系统在网络环境内外的信息保障程序，还可能包括采购职责。《框架》列出了该专业的30项具体任务，以及需要具备的23项KSAs。

（3）知识管理（Knowledge Management）：专业人员负责管理和控制使组织能识别、记录及访问智力资源和信息内容的流程和工具。《框架》列出了该专业的9项具体任务，以及需要具备的15项KSAs。

（4）客户服务与技术支持（Customer Service and Technical Support）：专业人员负责针对客户的需求和询问，追溯问题、安装程序、配置、故障诊断以及提供维护和培训。《框架》列出了该专业的14项具体任务，以及需要具备的13项KSAs。

（5）网络服务（Network Services）：专业人员负责安装、配置、测试、运行、维护和管理网络及其防火墙，包括各种硬件（集线器、网桥、交换机、多路复用器、路由器、电缆、代理服务器及配电保护系统）和软件，允许所有频谱传输信息的共享和传输，以支持信息和信息系统的安全性。《框架》列出了该专业的13项具体任务，以及需要具备的27项KSAs。

（6）系统管理（System Administration）：专业人员负责安装、配置、故障诊断和维护服务器配置（硬件和软件），以确保其机密性、完整性和可用性，管理账户、防火墙和补丁，负责访问控制口令（账户）的创建和管理。《框架》列出了该专业的17项具体任务，以及需要具备的23项KSAs。

（7）系统安全分析（Systems Security Analysis）：专业人员负责实施系统安全的集成/测试、运营和维护。《框架》列出了该专业的29项具体任务，以及需要具备的42项KSAs。

3.3 保护与防御

该大类专业领域负责鉴别、分析、减缓对内部IT系统或网络的威胁，包括五种典型专业岗位。

（1）计算机网络防御（Computer Network Defense）：专业人员负责收集各种来源的防御措施和信息，鉴别、分析并报告网络上发生或可能发生的事件，以保护信息、信息系统和网络免受威胁。《框架》列出了该专业的8项具体任务，以及需要具备的38项KSAs。

（2）应急响应（Incident Response）：专业人员负责对相关领域内的危机或紧要情况做出响应，以减缓当前及潜在的威胁。并根据需要，采用减缓、预备、响应和恢复方法来最大限度地提高生命生存、资产保护和信息安全，以及调查和分析所有相关的响应活动。《框架》列出了该专业的16项具体任务，以及需要具备的26项KSAs。

（3）计算机网络防护基础设施支持（Computer Network Defense Infrastructure Support）：专业人员负责测试、实现、部署、维护、管理那些被用来有效地管理计算机网络防护服务提供者网络和资源的基础设施硬件和软件，监控网络以主动纠正未授权的活动。《框架》列出了该专业的7项具体任务，以及需要具备的26项KSAs。

（4）安全程序管理（Security Program Management）：专业人员负责在组织、专项项目或者其他职责领域内管理相关安全（如信息安全）问题，包括：战略、人员、基础设施、策略强制执行、应急计划、安全意识普及和其他资源。《框架》列出了该专业的34项具体任务，以及需要具备的31项KSAs。

（5）漏洞评估和管理（Vulnerability Assessment and Management）：专业人员负

责在即时和非即时的环境下进行威胁和漏洞评估，确定与可接受配置、单位或本地策略的偏离，评估风险程度，开发和（或）建议合适的减缓措施。《框架》列出了该专业的7项具体任务，以及需要具备的26项KSAs。

3.4 调查

该大类专业领域负责调查IT系统、网络上的计算机事件或犯罪，以及数字证据，包括两种典型专业岗位。

（1）数字取证（Digital Forensics）：专业人员负责收集、处理、保存、分析并呈现计算机相关的证据，以佐证网络漏洞减缓和（或）犯罪、欺诈、反情报或执法调查。《框架》列出了该专业的29项普通任务和7项专门的执法/反情报任务，以及需要具备的32项普通KSAs和3项专门的执法/反情报KSAs。

（2）调查（Investigation）：专业人员负责将战术、技术和规程应用于全方位的调查工具和处理程序，包括但不限于：面谈和审讯手段、监视、反监视以及监视侦查，并能恰当地平衡起诉与获取情报的利弊。《框架》列出了该专业的22项具体任务，以及需要具备的12项KSAs。

3.5 作战与搜集

该大类专业领域负责高度专业化地搜集能用于情报工作的网络空间安全信息。包括两种典型专业岗位，但《框架》中未给出相应的具体任务和所需的KSAs。

（1）搜集活动（Collection Operations）：专业人员负责用适当的搜集策略，并以搜集管理过程中建立的优先级来执行情报搜集。

（2）网络作战计划（Cyber Operations Planning）：专业人员负责收集信息并制定详细的作战计划和命令以满足需求。为综合信息和网络空间作战活动，实施战略和战术级的全方位作战计划。

（3）网络作战（Cyber Operations）：专业人员负责使用自动化工具管理、监控和（或）实施大规模的网络作战活动以响应全国性的和战术的需要。

3.6 分析

该大类专业领域负责高度专业化地审查和评估面临的网络空间安全信息，以确定其情报价值。包括四种典型专业岗位，但《框架》中未给出相应的具体任务和所需的KSAs。

（1）网络威胁分析（Cyber Threat Analysis）：专业人员负责识别和评估网络犯罪分子和国外情报机构的能力和活动，提供裁决以便发起或支持强制执法和反情报的侦查或特别行动。

（2）全源情报（All Source Intelligence）：专业人员负责分析来自多源、多科目和情报界全部机构的威胁信息。综合并把这些情报信息连贯起来，提取出可能的含义或问题。

（3）深度分析（Exploitation Analysis）：专业人员负责分析搜集到的信息，以确定漏洞及其充分利用的潜在可能性。

（4）攻击目标（Targets）：专业人员负责致力于通晓一个或多个地区、国家、非国家实体以及（或）技术。

3.7 支持

该大类专业领域提供支持，以便保障其他人员能够有效地开展各自的网络空间安全工作，包括三种典型专业岗位。

（1）法律咨询和诉讼代理（Legal Advice and Advocacy）：专业人员负责在相关领域的各种相关问题方面，给领导和员工提供完整的法律意见和建议。或者，代表客户的利益，通过范围广泛的书面和口头工作（包含法律诉讼），提出法律和政策的变更并做出案例。《框架》列出了该专业的13项具体任务，以及需要具备的21项KSAs。

（2）战略规划和策略制定（Strategic Planning and Policy Development）：专业人员负责应用先验知识来定义企业（实体）的方针，决定如何分配资源，并确定在所涉范围内达到预期目标所需的流程或基础设施。制定策略或提出策略的变更以支撑新的措施或者所需的变化（增强）。《框架》列出了该专业的18项具体任务，以及需要具备的25项KSAs。

（3）教育和培训（Education and Training）：专业人员负责对相关领域内的人员进行培训。根据需要制定、计划、协调和评估培训课程、方法和技术。《框架》列出了该专业的21项具体任务，以及需要具备的16项KSAs。

4 结语

《NICE网络空间安全人才队伍框架（草案）》虽然还只是个初稿，不少细节方面有待商榷和完善，但从中可以看到美国在信息安全的全民化工作方面做得非常扎实，有充足的投入来开展信息安全人才培养的基础性工作，并能发动全国的力量参与其中。随着信息化（数字化）的发展，信息安全作为国家和社会所需的一种新兴专业和职业已经形成。END

参考文献：

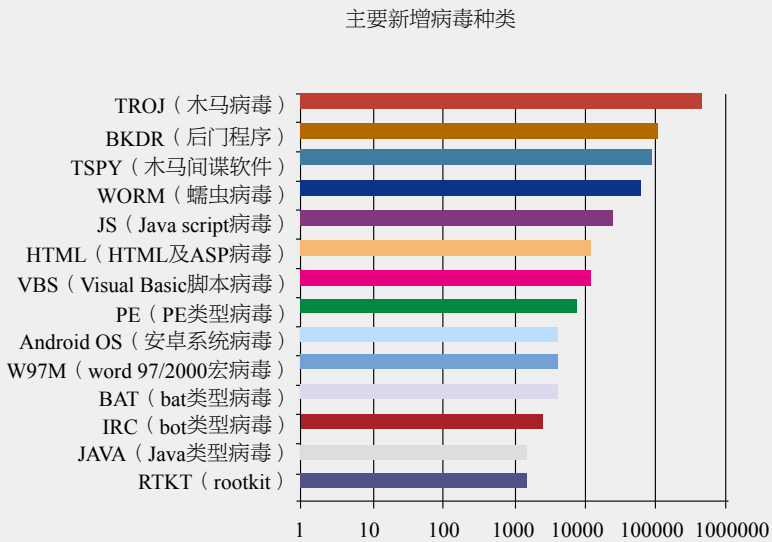
[1] National Initiative for Cybersecurity Education (NICE) Strategic Plan-Building a Digital Nation [R/OL].2011-08.http://www.nist.gov/nice/

[2] 韩臻,韩磊,马威.美国国家网络空间安全教育计划战略概述[J].保密科学技术,2012(07).

[3] NICE (National Initiative for Cybersecurity Education) -Cybersecurity Workforce Framework Summary [R/OL].2011-09.http://csrc.nist.gov/nice/framework/.

[4] NICE(National Initiative for Cybersecurity Education) -Cybersecurity Workforce Framework-printable [R/OL].2011-09.http://csrc.nist.gov/nice/framework/.

2012年第二季度中国地区新增病毒类型



（摘引自趋势科技发布的《2012年第二季度中国安全综合报告》）