信 息 化 研 究

2014 年第 24 期 总第 73 期

国家信息中心信息化研究部　　2014 年 12 月 24 日

英国政府信息安全经验与启示[1]

——英国政府信息化发展战略最新趋势与创新实践培训总结报告之二

王威[2]

【摘　要】英国政府高度重视信息安全工作，着力从组织架构、发展战略等方面建设国家层面的信息安全和保障体系。同时，英国将信息安全作为国家信息产业发展的一个重要领域，作为英国产业转型的一个重要方向着力发展。本报告在介绍英国政府信息安全经验的同时，针对我国情况提出了经验启示和工作建议。

【关键词】信息安全；英国；启示

1 报告资料来自培训考察及相关网站介绍。

2 王威，男，工学博士，国家信息中心信息化研究部战略规划研究室助理研究员，中国智慧城市发展研究中心首席工程师，研究方向为信息化发展战略、智慧城市顶层规划设计。

英国政府信息安全经验与启示

王威

2014 年 10 月，笔者随“英国政府信息化发展战略最新趋势与创新实践培训团”，深入了解了英国政府在推进信息安全工作中的组织模式和主要做法，并与英国政府相关人员进行了深入探讨。考察发现，英国政府的信息安全工作是紧紧围绕其国情和制度展开的，具有典型发展特色，并取得了比较显著的建设成效。英国信息安全建设经验，对于我国进一步推进信息安全体系发展具有良好借鉴意义。

英国政府认为，他们有义务使用安全可靠的信息通信技术来提供创新的公共服务，通过实现跨越多个组织的互联互通，确保市民和商业机构能无缝地访问所需的信息。英国政府强调安全有效地共享和使用信息是公共服务的核心内容，同时利用信息安全体系推动预防犯罪、改善社会环境以及有效应对网络恐怖主义等工作发展。

信息安全和保障（Information Security and Assurance，ISA）是英国提出的构建一个安全可靠的信息通信技术体系所需的过程和机制，借此让公民和公共服务部门能够安全地交换数据，通过改进互联互通水平使授权用户能够更稳定地跨部门访问信息，培育和塑造信息处理文化，增强公众对政府处理公民信息的信任度。

一、英国政府保障信息安全的主要机构

（一）网络安全与信息保障办公室

网络安全与信息保障办公室（The Office of Cyber Security & Information Assurance，OCSIA)在国家网络安全战略指导下，协调内政部、国防部、政府通信总部、国家基础设施保护中心、外交和联邦事务部、商务部等多个政府部门和机构，协同实施相应的网络安全计划。OCSIA 为内阁部长和国家安全委员会提供有关网络安全方面的决策支持，提供战略方向并协调政府的网络安全计划，增强英国的网络安全与信息保障。

OCSIA 与内政部、国防部、政府通信总部、电子通信安全部、国家基础设施保护中心、外交联邦事务部和商业、创新与技能部协同工作，负责实施一系列跨部门的议程。主要包括：提供包括网络犯罪在内的英国网络安全和信息保障的战略方向；支持教育、宣传、培训（如获得在线安全和网络安全挑战）；与私营部门合作伙伴开展信息交换和促进最佳实践；确保英国的信息与网络安全的技术能力和运行架构得到不断改进和维护；与政府资讯科技总监办公室协同工作确保政府公用网络和政务云等 ICT 基础设施的弹性和安全；与国际伙伴合作改进网络空间安全和信息安全等。

（二）政府通信总部

政府通信总部（Government Communications Headquarters，GCHQ）是英国最大的情报和安全机构，致力于运用专门知识和经验维护国家安全和通信安全，实现网络连接和基础设施的安全。GCHQ 下设通信与电子安全组（The Communications-Electronics Security Group，CESG），是 GCHQ 的信息安全部门，是英国国家信息安全保障的技术权威，在政府信息安全方面有决定性的发言权。

GCHQ 通过与工业界和学术界建立伙伴关系，并使用来自国家基础设施保护中心、军情五处和军情六处等单位对安全威胁的研判成果。GCHQ 一方面为政府的新建 IT 系统和现有 IT 系统的安全风险提供量身定制的建议，提供防范这些安全风险的思路和方案，同时与工业界合作建立标准和指南，确保政府部门使用适当的放心产品、服务和人员，并建立世界级的信息保障和网络安全专业人员库，以便政府部门利用并形成风险防范能力。此外，GCHQ 还对现有系统运行提供支持，如对特定的威胁和漏洞进行告警、提供应急响应以及保护数据的技术解决方案，如使用加密密钥保护最敏感的信息等。

CESG 为政府具体提供以下支持：保护政府的敏感信息和机密信息免受敌对威胁，以维护国家主权；作为政府 ICT 战略的一部分，确保公共部门内部使用 IT 的良好质量安全；作为政府数字化战略的一部分，确保政府与公民的在线互动；与工业界合作保护国家的关键基础设施。

（三）国家基础设施保护中心

英国政府将国家基础设施定义为“国家功能所必需的以及为英国公民日常生活提供基本服务的设施、系统、场站和网络”，并划分为：通讯、应急服务、能源、金融服务、食品、政府、健康、运输和水九大类。因此，国家基础设施保护

中心（The Centre for the Protection of National Infrastructure，CPNI）也是负责信息安全的重要部门。

CPNI 是保护国家基础设施的权威政府部门，为保护国家安全提供有关物理安全、人员安全、网络安全和信息安全保障等有关建议，以阻止和检测威胁。同时，CPNI 还资助各种保护英国网络空间国家利益、防范网络安全袭击等各类项目。

此外，英国还有内政部、国防部以及网络安全运行（作战）中心等政府机构从事与国家网络安全相关工作。

二、英国信息安全相关的国家战略

（一）国家安全战略

2010 年 10 月，英国政府发布国家安全战略报告《不确定时代一个强大的英国：国家安全战略》（A Strong Britain in an Age of Uncertainty: The National Security Strategy），将其他国家针对英国网络空间的敌对攻击和大规模网络犯罪列为国家面对的主要威胁之一。基于安全风险发生的可能性和影响程度，识别出了“恐怖主义、海外不稳定和冲突事件、网络安全、国内紧急事件、能源安全、有组织犯罪、边境安全、防扩散和军备控制”等八个主要方面。其中，高度重视“网络安全”的威胁，是四个“高优先级风险”之一（其他三个是国际恐怖主义、国际军事危机，以及因自然灾难或事故导致的国内紧急事件）。

（二）网络空间安全国家战略

2011 年 11 月，英国发布了网络空间安全的国家战略《大不列颠联合王国的安全战略：保护和提升数字世界中的大不列颠联合王国》（The UK Cyber Security Strategy-Protecting and promoting the UK in a digital world），主要阐述英国如何通过构建更为可信、更加弹性的数字环境以促进经济繁荣和保护国家安全。此战略提出了 2015 年实现四大目标的战略蓝图：一是有效应对网络犯罪，使英国成为全球网络空间开展业务最安全的地方；二是更为有效地抵御网络空间威胁，更好地保护网络空间的国家利益；三是致力于形成一个开放、稳定的网络空间，使公众能够安全使用并支撑一个开放的社会；四是具备支撑所有网络安全目标的跨领域知识、技巧和能力。

（三）网络空间安全国际战略

2012 年 9 月，英国贸易与投资署发布《网络安全，支撑英国出口的途径》

(Cyber Security, the UK's approach to export)，该战略致力于与全球范围的伙伴合作构建一个安全、稳健、开放和可信的互联网。

贸易与投资署希望将英国产业界推向全球网络安全供应基地的领导者，帮助有关国家应对网络犯罪、网络恐怖主义和国家级的谍报行动。报告阐述了网络安全作为英国出口拉动增长战略的基础部分的重要性，英国产业界的实力及其独特原因，发展机遇和市场分析，贸易与投资署的推进步骤，英国政府和工业界在出口战略中的各自角色，以及如何合作以实现出口增长，阐述了需要加以管理的相应风险。

报告对国际网络安全市场进行了分析，提出了以下框架：

图 1 网络安全市场分析框架

三、英国信息安全领域的部分措施

（一）制订实施安全政策指导性文件

2014 年，内阁秘书长、官方安全委员会（Official Committee on Security，SO）主席签署了英国政府的《安全策略框架》（The Security Policy Framework），提出了各安全领域的共同准则：

1、应反映英国最广泛的安全目标并确保英国政府最敏感的资产得到有效保护；

2、安全必须支撑政府业务并支持英国政府透明和公开的工作，通过适当的数字方式提供高效的服务；

3、风险管理是关键并应由决策层推进。通过评估，识别潜在的威胁、脆弱性和相应的措施，并将人员、信息和基础设施的风险降低到可接受的程度。这一过程将充分考虑相关的法定义务和保护，包括数据保护法案、信息自由法案、官方机密条例、平等法案，以及犯罪和警察法案等。

4、人员和行为是安全的基础。正确的安全文化、适当的期望和有效的训练不可或缺。

5、汇报、管理和解决任何安全事件都要有策略和程序，对系统崩溃或个人操作不当，将需要进行适当的处置。

（二）设置统一的政府网关

为便于公众更快找到自己想要的信息，英国建立了统一的政府信息门户网站，建立了统一的政府网关（Government Gateway），为个人、机构和代理等各种用户提供一站式登录和账号管理服务。

（三）提出网络防御的 20 项关键措施

国家基础设施保护中心（CPNI）发布了提高网络安全防御能力的 20 项关键措施：

1、编目管理设备权限。主动管理（编目、跟踪和纠正）网络上的全部硬件设备，确保只有授权设备能够访问，并发现和阻止未授权和不受管理的设备获得访问。

2、编目管理软件权限。主动管理网络上的全部软件，确保只有授权软件能

够安装和运行，发现和阻止未授权和不受管理的软件被安装和运行。

3、硬件和软件的安全配置。使用严格的配置管理和变更控制程序，建立、实现主动管理移动设备、便携电脑、工作站和服务器的安全配置，以防止攻击者利用脆弱的服务和设置。

4、持续评估和维护。持续的获取、评估新的信息并采取行动，以便识别和修补漏洞，尽量减少攻击者利用漏洞的机会。

5、防范恶意软件。在政府和企业多个位置控制恶意代码的安装、扩散和执行，同时优化部署自动化的快速更新防御、数据收集和纠正措施。

6、应用软件安全。管理所有自主开发和采购软件的安全生命期，以防止、检测和修正安全漏洞。

7、无线访问控制。跟踪/控制/预防/纠正安全使用无线局域网络（LAN）、接入点和无线客户端系统的过程和工具。

8、数据恢复能力。及时备份关键信息，并提供恢复数据的有效工具。

9、安全技能评估和培训。对于重要岗位，经常性评估其安全防御的专门知识、技能和能力；制定和执行综合评估计划，找出差距，并通过培训和宣传等进行持续改进。

10、防火墙、路由器和交换机等网络设备的安全配置。用严格的配置管理和变更控制流程来建立、实施和积极管理网络基础设备的安全配置，防止被攻击者利用。

11、网络端口、协议和设备的限制和控制。管理（跟踪/控制/纠正）网络设备正在使用的端口的协议和服务，以减少漏洞被攻击机会。

12、管理权限的控制。对计算机、网络和应用程序的管理权限的配置、分配和使用进行有效跟踪控制。

13、边界防御。检测、预防、纠正不同信任级别的网络信息流，并集中关注易被破坏的数据。

14、审计日志的维护、监视和分析。收集、管理和分析事件审计日志，以帮助检测和了解攻击并进行恢复。

15、控制访问。对人员、计算机和应用程序及其需要和有权访问的关键资产（信息、资源和系统等）进行正式分类和授权基础上，使用流程和工具来跟踪/控制/预防/纠正对关键资产的安全访问。

16、帐户监视和控制。主动管理系统帐户和应用程序帐户的整个生命周期，包括其创建、使用、休眠和删除，以减少被攻击机会。

17、数据保护。使用流程和工具防止数据泄露，减轻泄露数据的影响，确保敏感信息的隐私和完整性。

18、事件响应和管理。通过开发和部署事件响应基础架构（如：计划、角色定义、培训、沟通、监督管理）快速发现攻击并有效遏制损害、消除攻击者的存在，并恢复网络和系统的完整性。

19、安全网络工程。规划、设计和构建高可信系统运行的特征，使安全成为所有单位建设和运行重要准则。

20、渗透性测试和演练。通过模拟攻击行动测试系统的整体安全能力。

（四）建立信息保障联盟

建立英国信息保障联盟，其核心是通信与电子安全组 CESG，其他主要成员包括：内阁办公室、国家基础设施保护中心、信息委员会办公室（Information Commissioner’s Office，ICO）、国防部信息保障产品目录管理部门、网络安全与信息保障办公室（OCSIA）、政府采购服务（GPS）部门等。此联盟一方面协调上述部门的日常工作，同时代表英国政府参与有关国际联盟（如欧洲安全与合作组织、欧盟和世界经济论坛等）的日常活动。

四、英国政府信息安全工作对我国的启示

从英国构建信息安全保障体系的实践看，英国政府并未谋求在全球网络空间中的主导地位，而是将注意力集中在维护本国网络安全、加强本国网络安全产业竞争力、创造网络安全产业发展机遇等方面。

英国政府的主要措施是通过促进与信息安全相关部门的业务协同，制定操作性较强的、可执行的网络信息安全战略，为保障信息安全提供组织和制度的保障。

借鉴英国经验，我国首先应加快制定网络安全战略，将保障网络空间安全作为新时期维护国家利益的重要任务，制定切实可行的战略实施方案。其次要进一步加强国家网络安全与信息化领导小组对我国网络安全的统一领导和协调职责，提高保障网络安全、应对网络犯罪、推动网络应用和宣传推广等工作的协调能力。同时，在网络安全与信息化领导小组统一领导和协调下，加强各职能部门在信息安全领域的相互配合，确保我国网络安全战略的顺利实施。此外，应明确提出鼓励网络安全产业发展的政策、资金、法律等方面措施，推动我国网络安全企业做

大做强和安全产业快速发展，充分发挥网络安全产业在我国经济增长中的带动作用。

本期责编：马潮江　　**审稿：**武锋
联系地址：100045　北京市西城区三里河路 58 号　国家信息中心信息化研究部
联系电话：010-68557312　　电子信箱：macj@cei.gov.cn