

国家社会科学基金项目

主 编 周效坤 杨世松
副主编 韩文报 宋明武

信息反恐论

军事科学出版社

XINXI FANKONG LUN

国家社会科学基金项目

信息反恐论

主 编：周效坤 杨世松

副主编：韩文报 宋明武

编 委(按姓氏笔画排序):

丁 元	马晓军	王 涛	化长河
白炳泉	叶尔江	刘向明	阮 飞
杜永英	李 伟	吴松涛	吴绍民
张晓娟	陈 晨	邵广纪	杨 骥
周 林	袁风华	袁巍伟	高志诚
梁山华	韩 东	董红勋	樊伟中

军事科学出版社

图书在版编目(CIP)数据

信息反恐论/周效坤、杨世松主编. —北京:军事科学出版社,
2005.6

ISBN 7-80137-853-9

I. 信… II. ①周… ②杨… III. 信息技术-应用-反恐怖
活动 IV. D815.5

中国版本图书馆 CIP 数据核字(2005)第 042270 号

军事科学出版社出版发行

(北京市海淀区青龙桥/邮编:100091)

电话:(010)62882626

经销:全国新华书店

印刷:北京鑫海达印刷厂

开本:850×1168 毫米 1/32

版次:2005 年 6 月北京第 1 版

印张:12.875

印次:2005 年 6 月第 1 次印刷

字数:300 千字

印数:1-3000 册

书号:ISBN 7-80137-853-9/E·572

定价:21.00 元

《信息反恐论》专家鉴定组

组长：何德全(中国科学院院士，国家信息安全著名专家)

成员(按姓氏笔画排序)

王保存(军事科学院研究员，信息战专家，少将)

吴世中(国家信息技术安全测评论证中心主任，国务院信息办专家组成员)

周仲义(中国工程院院士，少将)

修光亚(研究员，总装备部信息安全专家组成员)



序

《信息反恐论》是解放军信息工程大学课题组承担的国家社会科学基金项目。该课题组成员曾承担并公开出版全军军事科研“十五”计划课题《信息国防论》，可以说，《信息反恐论》是《信息国防论》的姐妹篇。这是信息化建设中一件有重要意义的工程。课题组要我作序。我仔细阅读了该书，写一点感想。

在信息时代，恐怖分子的活动范围扩大，已开始利用各种信息工具从事恐怖活动，这就是信息恐怖主义。美国联邦调查局特别调查处的马克·帕尼特把电脑恐怖主义定义为“由亚国家组织或秘密人员有预谋、有政治目的地对信息系统、计算机系统、计算机程序及数据所实施的攻击，这种攻击可导致对非战斗目标的暴力”。它是一种软杀伤力，对人们心理产生的恐惧效果与暴力恐怖产生的效果一样，有时甚至更甚。信息恐怖活动介于滥用信息系统或用信息系统实施欺骗的犯罪行为与有形的暴力恐怖活动之间，常通过滥用一个数字化信息系统、网络或其中的一部分来实施恐怖活动，或使其行为更加方便。

该研究课题分3篇。第一篇用4章概述了信息恐



怖活动的基本内容、特征、活动方式、作用机制及主要手段；第二篇用4章介绍了信息反恐怖的技术体系，主要是监控与防范技术、预防与抗攻击技术、防病毒与防黑客技术、数据库安全技术；第三篇用7章的篇幅，系统地论述了营造信息反恐怖的环境、确定信息安全战略、推进联合信息防御和信息系统的防范、加强信息反恐怖管理和信息反恐基础建设，还介绍了发达国家对付信息恐怖的措施。该研究成果结构合理，内容也较完整，有理论创新，其对策措施操作性也强，对开展信息反恐怖有一定的指导价值。

反对信息恐怖，确保信息安全已成为世界主要国家普遍关注的重大国家战略。1998年12月，联合国大会通过了53170号决议，与会所有成员国就信息安全、反击信息恐怖主义和犯罪以及如何采取措施等问题交换了意见。这种国际反恐与合作正进一步加强。

要大力增强信息反恐意识，普及信息反恐教育。在信息时代，需要综合运用经济手段、政治努力、强有力的军事和道德行为准则，来反击恐怖分子运用信息手段和信息技术进行信息恐怖活动。我国信息安全战略目标 and 任务是：适应信息技术、信息安全环境的变化，适应国家信息化发展和国家安全战略的要求，完善信息安全保障体系，提高保护防范、监测监控、应急响应和积极防御能力，为促进国民经济发展，维护社会稳定、国家安全和个人合理流动权益提供信息安全保障。



信息安全已成国家安全的重点之一。构筑信息反恐长城，确保信息安全，为全面建设小康社会提供坚实基础，这是一项长期的任务。防范信息恐怖、保障信息安全，不仅要发展信息安全技术与产品，还要完善和强化整个社会的法律体系、安全意识、人才保障、道德观念、管理水平、危机管理机制等，逐步形成—个政府宏观调控和科学引导、企业积极配合、全社会广泛参与的信息安全保障体系。

2004年10月28日



第一篇 概述篇

第一章 恐怖活动是威胁人类安全的“政治瘟疫”	(2)
一、恐怖与恐怖活动	(2)
(一) 恐怖活动的内涵	(2)
(二) 恐怖活动的新特点	(3)
二、恐怖活动的类型和手段	(6)
(一) 传统恐怖活动	(6)
(二) 新型恐怖活动	(9)
(三) 超级恐怖活动	(17)
三、恐怖活动的危害和根源	(20)
(一) 恐怖活动的危害	(20)
(二) 恐怖活动的根源	(23)
四、反恐怖斗争是国家安全的重要内容	(37)
(一) 反恐怖是现代国防的重要内容	(38)
(二) 反恐怖斗争逐渐成为维护国家安全的 立足点	(39)
第二章 信息恐怖是危害更大的恐怖活动	(42)
一、信息恐怖活动的出现及前提条件	(42)
(一) 信息恐怖活动的出现	(43)



(二) 信息恐怖活动的前提条件	(45)
二、信息恐怖主义的基本含义及相关范畴	(48)
(一) 计算机化激进主义与信息恐怖主义	(49)
(二) 黑客行动主义与信息恐怖主义	(50)
(三) 计算机犯罪与信息恐怖主义	(51)
(四) 信息恐怖活动是信息战的一种类型	(53)
三、信息恐怖活动的组织形式及特征	(56)
(一) 信息恐怖活动的组织形式	(56)
(二) 信息恐怖活动的特征	(58)
四、信息恐怖主义的活动方式	(63)
(一) 利用互联网加强恐怖主义宣传和扩大恐怖组织	(63)
(二) 以信息和网络设施为破坏目标	(64)
(三) 运行机制机动灵活	(65)
五、信息领域反恐怖是各国人民面临的重要任务	(66)
(一) 信息恐怖主义有进一步泛滥的趋势	(66)
(二) 恐怖主义集团的网络化要求反恐的 国际合作	(67)
第三章 信息恐怖的主要类型及作用机制	(69)
一、黑客及其攻击行为	(69)
(一) 黑客的信息恐怖行为	(70)
(二) 黑客攻击行为的主要手段	(71)
(三) 黑客信息恐怖的特点及危害	(73)
二、病毒及其攻击模式	(74)
(一) 计算机病毒的产生及分类	(74)
(二) 计算机病毒的传播途径与生命周期	(76)
(三) 计算机病毒是危害极大的信息恐怖	(78)
三、信息恐怖的作用机制和领域	(80)



(一) 信息恐怖的作用机制	(80)
(二) 信息恐怖的作用领域	(82)
第四章 信息恐怖活动的主要手段	(86)
一、信息污染与信息欺骗	(86)
(一) 信息污染	(86)
(二) 信息欺骗	(90)
二、信息遮断与信息封锁	(92)
(一) 信息遮断	(92)
(二) 信息封锁	(95)
三、信息窃取与信息破解	(97)
(一) 信息窃取	(97)
(二) 信息破解	(101)
四、信息威慑与实体摧毁	(102)
(一) 信息威慑	(102)
(二) 实体摧毁	(103)
第二篇 信息反恐怖技术篇	
第五章 网络恐怖入侵的检测与预防技术	(108)
一、网络恐怖入侵的检测技术	(108)
(一) 入侵检测概念	(108)
(二) 入侵检测系统类型	(110)
(三) 常用检测方法	(115)
(四) 入侵检测系统选择	(116)
(五) 入侵检测技术的发展方向	(117)
二、网络恐怖的入侵预防技术	(119)
(一) 网络入侵预防	(119)
(二) 入侵隔离技术	(123)



第六章 抗黑客攻击技术	(127)
(08) 一、安全操作系统	(127)
(08) (一) 操作系统安全是系统安全的基础	(127)
(08) (二) 操作系统安全模型与安全评估准则	(130)
(08) (三) 我国安全操作系统所面临的问题及	(131)
(00) 发展对策	(131)
(50) 二、网络加密技术	(133)
(50) (一) 加密的基本方法	(133)
(50) (二) 密钥管理技术	(134)
(70) 三、信息认证技术	(136)
(70) (一) 口令鉴别	(137)
(101) (二) 信物鉴别	(139)
(501) (三) 生物特征鉴别	(139)
(501) (四) 数字签名技术	(140)
(501) (五) 报文鉴别	(141)
(六) 证书鉴别 (GA)	(142)
四、信息过滤技术	(143)
(一) 防火墙	(143)
(801) (二) 垃圾邮件过滤器	(146)
(8.1) (三) 网页过滤器	(148)
(801) 五、安全审计技术	(149)
(011) (一) 安全审计过程	(149)
(211) (二) 安全审计技术	(150)
(011) (三) 审计跟踪实施	(151)
(51) 六、无线网络抗恐怖攻击技术	(153)
(011) (一) 抗恐怖攻击基础技术	(154)
(011) (二) 新的无线网络安全标准	(156)
(551) —IEEE802. 11i	(156)



(001)	(三) 动态安全链路 (DSL) 技术	(157)
(101)	(四) 虚拟专用网 (VPN) 技术	(159)
	第七章 反病毒攻击技术	(161)
(501)	一、病毒的预防、检查和消除	(161)
(103)	(一) 病毒的预防	(161)
(104)	(二) 病毒的检查	(166)
(105)	(三) 病毒的消除	(172)
(107)	二、网络病毒的防范	(175)
(300)	(一) Novell 网的病毒预防	(175)
(300)	(二) WindowsNT 网络的病毒防范	(176)
(303)	(三) 预防网络病毒的措施	(177)
(305)	三、反病毒技术	(178)
(308)	(一) 实时反病毒技术	(178)
(309)	(二) 32 位内核技术	(179)
(304)	(三) VxD 机制	(180)
(307)	(四) 无缝连接	(180)
(308)	(五) 虚拟机技术	(181)
(305)	(六) 主动内核 (Active K) 技术	(182)
(309)	(七) 检查压缩文件病毒技术	(182)
(101)	四、反病毒工作中的对策	(183)
	(一) 防病毒工作所面临的新问题	(183)
	(二) 病毒防治的对策	(183)
	(三) 防病毒产品的开发原则	(184)
	第八章 数据库安全防范技术	(186)
(110)	一、数据库系统的入侵防护技术	(187)
(314)	(一) 口令管理	(187)
(115)	(二) 用户分类授权和存取控制	(188)
(115)	(三) 身份认证	(189)



(四) 数据库完整性检测和数据隔离	(190)
(五) 漏洞扫描	(191)
(六) 审计跟踪和攻击检测	(192)
(七) 操作系统防护和网络防护	(192)
二、数据库系统的安全加密技术	(193)
(一) 数据库安全技术	(194)
(二) 数据库加密的目的和要求	(195)
(三) 数据库加密技术	(197)
三、数据库系统的反摧毁技术	(200)
(一) 数据库系统的管理技术	(200)
(二) 数据库容错技术	(202)
(三) 数据库中间件技术	(202)
(四) 主动监测技术	(203)
(五) 身份取证技术和攻击陷阱技术	(203)
四、数据库系统的备份和恢复技术	(204)
(一) 数据库系统备份的目的	(205)
(二) 备份介质的选择和比较	(206)
(三) 备份技术	(207)
(四) 备份策略和备份方式	(209)
(五) 灾难恢复	(210)

第三篇 对策篇

第九章 积极防御, 确定国家信息安全战略	(214)
一、信息安全战略是国家安全战略的核心	(214)
(一) 信息时代的国家安全观	(214)
(二) 中国面临的信息安全形势和威胁	(218)
(三) 确定积极防御型的信息安全战略	(220)



二、国家信息反恐体制架构	(226)
(一) 国家组织体系	(226)
(二) 运行机制	(229)
(三) 法规管理	(230)
三、角逐信息战场, 捍卫网络疆土	(234)
(一) 制信息权是赢得信息反恐的关键	(234)
(二) 建设信息系统防护技术体系	(237)
(三) 建设有自主知识产权的信息安全保障 体系	(239)
第十章 打牢根基, 全面加强信息反恐基础建设	(243)
一、信息反恐怖基础设施建设方略	(243)
(一) 重视信息技术基础的建设, 特别是智能型 基础设施的建设	(244)
(二) 强化和发挥信息资源的开发与管理 功能	(245)
(三) 努力扫除“信息盲”, 提高全社会的 信息能力	(246)
(四) 保卫信息文化主权, 加强治理信息 环境	(247)
(五) 切实加强对关键信息网络系统即信息 基础设施保护	(247)
(六) 建立关于信息反恐怖基础设施安全状态的 国家级和地方级的数据库	(248)
(七) 把信息反恐怖斗争建立在自主产品和 核心技术基础上	(249)
二、信息反恐怖法规建设	(249)
(一) 信息反恐怖法规建设的含义和目标	(250)
(二) 信息反恐怖立法的措施	(251)



(355)	(三) 信息反恐怖立法的基本框架和内容·····	(253)
(355)	三、信息反恐怖动员体系·····	(256)
(355)	(一) 营造反恐怖信息环境, 完善信息反恐怖动员	
(355)	体系·····	(256)
(355)	(二) 加强信息反恐怖法规的教育与实施·····	(257)
(355)	(三) 重视网络政治动员与信息软权力的威胁, 构筑	
(355)	多维度信息反恐怖安全战略·····	(259)
	四、信息反恐怖的人才建设·····	(262)
(355)	(一) 培养信息反恐怖人才的现实意义和	
(355)	历史紧迫感·····	(262)
(355)	(二) 对信息安全人才素质的基本要求·····	(264)
	(三) 跨越式培养信息反恐怖人才·····	(266)
	第十一章 严密组织, 营造信息反恐环境·····	(272)
	一、强化信息安全管理·····	(272)
(355)	(一) 信息安全管理的制约因素·····	(272)
	(二) 信息安全管理的的基本要求·····	(273)
(355)	二、开展信息安全督查·····	(277)
	(一) 掌握信息恐怖活动规律·····	(277)
(355)	(二) 强化信息安全检查·····	(278)
	三、消除信息安全隐患·····	(279)
(355)	(一) 防范外界环境的影响·····	(280)
	(二) 评估信息系统的缺陷和脆弱性·····	(280)
(355)	(三) 完善早期预警和安全监测功能·····	(282)
	(四) 堵塞信息保密管理漏洞·····	(283)
(355)	四、控制信息资源分配·····	(284)
(355)	(一) 开发利用信息资源·····	(284)
(355)	(二) 控制信息资源分配·····	(286)
(355)	(三) 加强信息资源管理·····	(287)



五、营造有利环境, 打击信息恐怖行为	(288)
(一) 抢占制高点, 构筑信息反恐怖的技术 平台	(288)
(二) 树立防范意识, 营造打击信息恐怖 氛围	(289)
(三) 开展全民教育, 增强群众性信息反恐怖 基础	(290)
(四) 加强监管, 净化信息安全环境	(291)
第十二章 整体保护, 确保信息系统安全	(293)
一、信息获取系统安全的防范	(293)
(一) 信息源保护	(293)
(二) 信息获取过程安全防护	(296)
二、信息传输系统安全的防范	(297)
(一) 信息加密	(298)
(二) 用户识别、控制与管理	(298)
(三) 网络安全	(300)
三、信息处理系统安全的防范	(303)
(一) 外部连接环境保护	(304)
(二) 信息处理平台保护	(309)
(三) 信息处理过程保护	(313)
四、信息存储系统安全的防范	(314)
(一) 数据库管理系统的安全保护	(314)
(二) 系统信息容灾	(315)
(三) 数据环境安全保护	(316)
(四) 数据审计控制与标识鉴别	(316)
第十三章 措施有力, 强化信息安全管理	(318)
一、技术安全管理措施	(318)
(一) 网络安全管理	(318)



(二) 密钥的管理	(322)
(三) 软件和设备的管理	(322)
二、行政管理措施	(325)
(一) 安全组织机构	(325)
(二) 安全人事管理	(327)
(三) 应急管理	(328)
三、物理环境管理措施	(329)
(一) 物理环境管理原则	(329)
(二) 防电磁泄漏措施	(330)
(三) 防微波炸弹措施	(334)
第十四章 综合保障, 推进联合信息防御	(338)
一、联合信息防御的指挥体系	(339)
(一) 国家信息防御指挥体系的组成	(339)
(二) 联合信息防御的指挥机制	(344)
(三) 国家信息反恐怖力量体系	(345)
二、联合信息防御的综合保障体系	(347)
(一) 联合信息防御的战略保障体系	(348)
(二) 联合信息防御的评价保障体系	(351)
(三) 联合信息防御情报保障体系	(352)
(四) 联合信息反恐怖的社会心理保障体系	(353)
三、国际信息反恐怖的合作机制	(355)
(一) 国际信息反恐怖联盟的建立	(355)
(二) 国际信息反恐怖的合作机制	(356)
第十五章 经验借鉴, 研究发达国家信息反恐怖 (三)	
措施	(357)
一、把反信息恐怖提到国家战略的高度	(358)
(一) 美国的四大国家战略	(358)
(二) 《打击恐怖主义国家战略》的主要内容 ...	(359)