

GANGKOU SHESHI BAO'AN

CONGYE RENYUAN GANGWEI PEIXUN JIAOCHENG

港口设施保安

从业人员岗位培训教程

第 2 版

交通运输部水运科学研究院 编

人民交通出版社

北京

GANGKOU SHESHI BAO'AN
CONGYE RENYUAN GANGWEI PEIXUN JIAOCHENG

港口设施保安
从业人员岗位培训教程
(第2版)

编写委员会 >>>

主 编:丁 倩 陈 朝

编 委:朱建华 梁 克 徐宏伟 褚冠全

樊洪涛 卢 新 占小跳 李 筠

张 霞 孟 于 梁 瑶 李世明

焦凌希 陈 实 韩棒棒 范湘丰旭

唐思远 陈 智 刘楠楠 林军保

王爱学 钱满清 刘大勇 邓红文

李志萍 陈成鑫 陈志雄 曹雪飞

张宗晏

编写单位简介 >>>

(一)交通运输部水运科学研究院

交通运输部水运科学研究院(以下简称“水运院”)成立于1956年,是中国成立最早、规模最大的水路交通运输科研机构,也是唯一的综合性水路交通运输科研机构。作为交通运输部直属一级科研事业单位,水运院多年来在智慧港口及智能航运技术、船舶溢油及危化品泄漏事故风险防范与应急技术、沿海和内河船舶污染综合防治技术、船舶防污染国际公约跟踪及研究、水运安全管理技术、水运安全风险与防控、水上交通工程、航海保障技术、水运应急与决策支持等方面开展了大量的工作,形成了以“水运经济、安全应急、环保节能、现代物流、智能水运”五大科研领域为主、基本全面覆盖水路交通运输各个方向的专业体系,集咨询服务、装备研发、工程设计、航运服务、交流培训五大产业板块于一体的业务领域。

目前,水运院现有7个机关职能部门、14个院属机构、3个院管单位,18个院属企业(含控股)、1个博士后科研工作站,挂靠有3个全国标准化技术委员会及分支机构、5个中国航海学会分支机构、7个专业工作机构。水运院总占地面积约17.2万平方米,建筑面积约6.6万平方米,在大兴拥有一座占地208亩的大型综合性实验基地,在黄河小浪底库区建有1000余亩的洛阳华洋生态科技园,在天津和青岛正在规划建设海上溢油应急处置实验基地和智能航运研发基地。建有1个国家国际科技合作基地(水路运输污染防治与重特大事故应急技术国家国际科技合作基地)、3个交通行业重点实验室、5个院级重点实验室和3个政府决策支持平台。水运院高层次人才培养力度不断加大,人才储备体系初步建立。其中,第三届交通运输部专家委员会委员3人,享受国务院政府特殊津贴8人次,交通运输部“新世纪十百千人才工程”第一层次人才3人,首批新世纪百千万人才工程国家级人选2人,交通运输青年科技英才12人,交通运输部科技创新领军人才2人,航海学会科技贡献突出人物5人,航海学会青年科技人才3人,院首席研究员3人,院青年首席研究员12人,院青年科技英才19人,历年入选国家和省部级专家库200余人次。

(二)科学技术交流与合作中心(港口标准化研究中心)

科学技术交流与合作中心(港口标准化研究中心)是水运院报经交通运输部批准组建的专业研究机构。中心牢牢把握科研机构职责定位,以“立足科研,服务政府与行业”为

目标,牵头承担港口标准化研究、人才发展研究、技术培训、技术交流合作推广等业务,着力打造高端技术交流平台 and 标准化研究平台。服务国家标准化管理委员会、交通运输部等政府部门,并承担全国港口标准化技术委员会秘书处、港口设施保安履约工作组秘书处等职能。

经过多年的发展与建设,中心打造了一只朝气蓬勃的研究团队,中心专业技术人员中,副高级以上技术职称占 30% 以上,硕士以上学历占 70% 以上。中心积累了优良的业绩,科研咨询服务对象遍及全国各地港航管理部门及企事业单位。中心建有设备配套齐全的视频教室,开发了网上直播平台 and 培训手机应用软件(App),依托院国家级国际科技合作基地、北京大兴实验基地、天津滨海实验基地、青岛智能航运研发基地等科研基础条件,依靠院专业门类齐全、专家资源丰富的优势,中心开设了各类技术培训,举办了多起公益专家讲座,课程广受欢迎。

我们的优势

- (1)专业的技术保障;
- (2)政府与企业沟通的桥梁;
- (3)港航人员交流的平台。

我们的服务

- (1)专业培训:面向港航管理部门 and 企事业单位,根据行业需求开发的水运类公开课程。
- (2)培训咨询:面向港航管理部门 and 企事业单位,根据客户需求和客户特点提供有针对性的培训咨询。
- (3)公开讲座:面向港航管理部门 and 企事业单位,就行业关注的热门话题展开分析与讨论。
- (4)行业交流:依托全国港口标准化委员会开展系列活动和学术论坛。
- (5)国际交流:依托国家财政支持的各类对外援助培训项目及国际会议,面向港航管理部门 and 企事业单位搭建国际交流平台。

GANGKOU SHESHI BAO'AN
CONGYE RENYUAN GANGWEI PEIXUN JIAOCHENG

港口设施保安
从业人员岗位培训教程
(第2版)

前言 >>>

2002年12月,国际海事组织通过了《1974年国际海上人命安全公约海上保安修正案》和《国际船舶港口设施保安规则》。根据公约和规则的要求,我国在2004年7月1日公约修正案生效时如期履约。我国履约工作开展近二十年来,已逐步建立起港口设施保安的长效机制,取得了显著成果,得到了国际社会的普遍认可。

为推动港口设施保安工作的进一步开展,我院科学技术交流与合作中心在二十余年从事港口设施保安研究及培训工作的基础上,结合《中华人民共和国港口设施保安规则》的要求和当前港口设施保安工作实际,根据《港口设施保安从业人员岗位培训结业测试大纲》,组织专家和技术人员第七次修订《港口设施保安从业人员岗位培训教程》。全书共分为两篇,第一篇为基础知识,第二篇为管理实务。本书可以作为港口设施保安管理及从业人员理解和掌握我国港口设施保安发展及实际操作的指导用书,也可以作为港航管理部门及港口企业实施港口设施保安管理培训的教材。

编者
2024年2月

目录 >>>

第一篇 基础知识

单元一 恐怖主义与港口设施保安	3
模块一 恐怖主义概述	3
模块二 港口设施保安概述	15
单元二 港口设施保安法规及标准	36
模块一 港口设施保安相关法律法规、部门规章及文件	36
模块二 港口设施保安技术标准	56

第二篇 管理实务

单元一 潜在保安威胁事件类型及应对措施	71
模块一 潜在保安威胁事件的类型	71
模块二 典型码头针对潜在保安威胁事件的应对措施	74
单元二 港口设施保安评估及计划报告编制要求	80
模块一 港口设施保安评估编制要求	80
模块二 港口设施保安计划制订要求	94
单元三 港口设施保安培训、训练及演习	102
模块一 人员配置与培训	102
模块二 港口设施保安训练及演习	108
单元四 《港口设施保安符合证书》申请核发及年度核验实务	131
模块一 《港口设施保安符合证书》申请核发	131
模块二 年度核验的申请程序、内容与方法	133
单元五 港口设施保安设备设施及技术	154
模块一 周界保安设备设施及技术	154
模块二 通道控制保安设备设施及技术	156
模块三 保安检查设备设施及技术	160
模块四 保安监控设备设施及技术	175

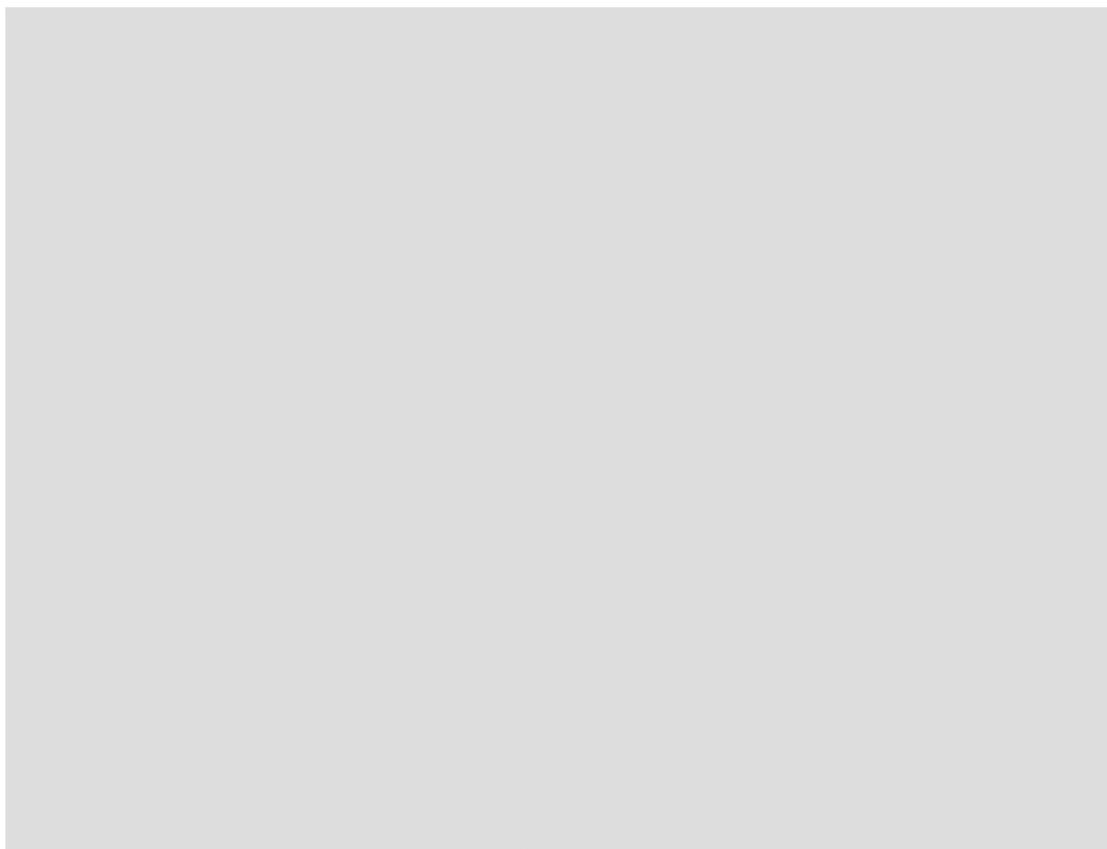
模块五 保安通信设备设施	180
附录	182
附录1 港口设施保安从业人员岗位培训结业测试大纲	183
附录2 单元模拟练习题答案	187

GANGKOU SHESHI BAO'AN
CONGYE RENYUAN GANGWEI PEIXUN JIAOCHENG

港口设施保安
从业人员岗位培训教程
(第2版)

——»» 第一篇

基础知识



单元一 恐怖主义与港口设施保安

模块一 恐怖主义概述

一、恐怖主义的定义

“恐怖主义”一词的定义一直存在争议。鉴于定义该词时政治立场和情感态度不同,国际社会对恐怖主义罪行定义一致性的进程一直停滞不前。

(一) 词典定义

恐怖主义的英文翻译为 Terrorism, 是 Terror(恐怖) + ism(主义)的合成词。

《韦氏大词典》^①认为:恐怖主义是①系统地使用恐怖行为,特别是作为一种胁迫的手段;②使用暴力行为恐吓一个地区的人民,以此作为试图实现政治目的的一种方式。这个定义阐明了恐怖主义是以“强迫”为手段,也就是现在大多数定义中所强调的暴力或者以暴力相威胁为手段,而且也指出来恐怖主义的目的在于试图实现政治目的。

《简明不列颠百科全书》^②对恐怖主义的解释是:恐怖主义是对各国政府、公众或个人使用令人莫测的暴力、讹诈或威胁,以达到某种特定目的的政治手段。各种政治组织、民族团体、宗教狂热者等,以及军队和秘密警察都可以利用恐怖主义。这个定义指出了恐怖主义的三个特征:①恐怖主义的打击目标是各国政府、公众、或个人;②恐怖主义是达到某种特定目的的政治手段,这种手段主要是使用令人莫测的暴力、讹诈或威胁;同时,恐怖主义的暴力具有很大的隐蔽性、突发性,总是在人们意想不到的时间和地点,发动突然的袭击;③恐怖主义的主体是各种政治组织、民族团体、宗教狂热者等。但没有将国家列举出来,不够全面。

《布莱克维尔政治学百科全书》^③认为:恐怖主义可以简洁地定义为强制性恐吓。或者更全面地定义为系统地使用暗杀、伤害和破坏,或者通过威胁使用上述手段,以制造恐怖气氛,宣传某种事业,以及强迫更多的人服从于它的目标。

《美国传统大学辞典》(American Heritage College Dictionary)^④对恐怖主义的解释是:对武力或暴力的非法使用或威胁使用,一个人或一个有组织的集团以威胁或胁迫社会或政府为目的而危害人类或财产,常带有意识形态或政治原因。这个定义突出的是:一是明确指出政

① 引自 <https://www.merriam-webster.com>。

② 引自《简明不列颠百科全书·第四卷》第817页(中国大百科全书出版社,1985年10月)。

③ 引自《布莱克维尔政治学百科全书》(中国政法大学出版,2002年)。

④ 引自《美国传统大学辞典》第1854页(霍顿米夫林出版公司,1996年)。

治目的,二是指出实施恐怖主义行为的原因,三是明确指出恐怖行为可能造成的危害。

(二)规约或立法定义

不同的国际组织和国家对恐怖主义采用不同的定义。

在20世纪70~80年代,联合国曾经试图对此作出定义,但各成员国在对待民族解放和民族自决所引起的冲突而使用暴力的态度上有分歧,最终不了了之。这些分歧使联合国不能订立包含单一、全面、具法律约束力的恐怖主义定义在内的《关于国际恐怖主义的全面公约草案》。联合国就恐怖主义的定义组织讨论过多次,至今仍无一致的意见。自1994年,联合国大会再三以这样的言辞谴责恐怖活动:“企图引起公众恐慌的犯罪行为,不管是个人还是团体为追求政治目的而从事这些行为都是不可接受的,不管其背后的性质是政治、意识形态、哲学、种族、宗教等都不能使之合法化”。通过联合国的多次讨论,目前基本形成了一种倾向性的意见,即承认恐怖主义定义有三要素:非法暴力、具有政治动机、滥杀无辜。

《美国法典》(United States Code)第22篇第2656f(d)节有关恐怖主义的定义:“恐怖主义”一词指由次国家组织或秘密团伙人员对非作战目标采取有预谋的、有政治动机的暴力行动。

2001年9月19日欧盟委员会通过两项法案,明确界定了欧洲范围内恐怖主义行为的概念和对相关罪行的量刑标准。有关打击恐怖主义行为的法案规定,恐怖主义行为的概念是个人或组织故意针对一个或多个国家,或针对被侵犯国家的机构和人民进行旨在威胁、严重破坏甚至摧毁政治、经济和社会组织及其建筑物的行为。

二、恐怖主义的历史

恐怖活动作为人类冲突的一种表现形式,有着悠久的历史。细究起来,恐怖活动应能追溯到古希腊和古罗马时期。古希腊历史学家色诺芬就曾专门记述过恐怖活动对敌方居民造成的心理影响。中国古代的荆轲刺秦王、古罗马的恺撒大帝遇刺都是历史上发生过的恐怖事件。美国总统肯尼迪被刺身亡是当代历史中的典型恐怖主义事件。

“恐怖主义”一词最早出现在18世纪法国大革命时期。为保卫新生政权,国民公会通过决议,“对一切阴谋分子采取恐怖行动”。由此我们不难看出恐怖主义不是一般的、孤立的、偶然的恐怖行动,而是指一种有组织、有制度和有政治目的的恐怖活动。

18世纪以前,恐怖活动基本上以暗杀、投毒为主要表现形式,恐怖活动多发生于各国国内。18世纪末到第二次世界大战结束时期发生了两起极为严重的恐怖事件,1881年沙皇亚历山大二世遇刺和1914年奥匈帝国斐迪南大公遇刺。实施者都是在没有群众支持的情况下,通过谋杀某一政府要员向社会宣传自己的政治目的,吸纳民众参与。

19世纪恐怖活动开始超越国界,国际化趋势日益显著。国际恐怖主义的真正形成是在第二次世界大战之后到20世纪60年代末这一时期。1968年发生的142起国际恐怖事件,标志着战后20多年相对安宁的时期结束,各种世界权威机构均将该年视为对当代国际恐怖活动数量和类型进行统计和分类的起始年。在此期间,恐怖主义的活动热点是在殖民地、附属国或刚独立的民族国家,这一时期的恐怖事件明显增多,手段日趋多样,如劫机、爆炸、绑架与劫持人质,袭击目标和活动范围已经超出国界,越来越具有国际性,逐渐形成了国际恐怖活动。

20 世纪 70 年代以后,恐怖主义组织已经形成一个较为松散的国际网络。据美国著名的智囊机构兰德公司的有关资料,20 世纪 80 年代全世界共发生了近 4000 起恐怖活动,比 20 世纪 70 年代增加了 30%,死亡人数则翻了一番。

据有关研究国际恐怖活动的机构统计,在 1970 年到 1979 年的 9 年间,因遭恐怖活动丧命的人数多达 4000 人,年均 400 余人;1988 年国际恐怖活动发生了 856 起,死亡人数多达 660 人,其中中东地区因民族矛盾比较复杂,共发生 313 起,占全世界恐怖活动的 36%,是恐怖活动的多发地区。

进入 20 世纪 90 年代以后,恐怖活动有了明显的变化,老的恐怖组织开始逐步退出历史舞台,新的组织开始出现。联合国发表的一份关于“全球恐怖活动状况”的报告显示,1997 年全球恐怖活动再次增多,高达 560 起,死亡 420 人。报告称:“国际恐怖活动中死亡的人数增加,是因为恐怖活动日趋残酷地袭击无辜平民并使用爆炸力更大的炸药或炸弹。”与此同时,报告强调:“恐怖行为更具隐蔽性和杀伤性”。恐怖事件发生后,再也没有人像过去那样站出来声称对事件负责,是 20 世纪 90 年代国际恐怖主义的一个最为显著的特点。发动者发现保持神秘也是一种武器,其恐怖作用高于以往的声张。像美国驻东非使馆在 1998 年 8 月 17 日被炸,至今还没有人声称对其负责,就是一个很好的例子。恐怖主义不断与民族分裂主义、宗教极端主义、无政府主义等众多极端主义互相交织,形成了关系密切的庞大势力。

进入 21 世纪后,恐怖势力彻底从过去的中东、拉美等主要地区蔓延到全球的各个国家。这些年里,许多恐怖组织的活动范围不断扩大,袭击的手段也不断更新和增加,其中包括爆炸、劫持、生化武器、网络恐怖主义等,手段极其血腥残暴。各国面临的恐怖主义威胁越来越严重,而恐怖主义也越来越成为一个需要世界各国共同努力进行打击的一项任务。不少研究恐怖主义的人士认为“恐怖主义将是 21 世纪威胁人类生存的主要敌对力量”。

三、恐怖袭击的主要手段

当今恐怖活动的类型和手段呈多样化发展趋势,既有传统手段,也有非传统手段。既有针对国家的政治性恐怖活动,也有针对社会团体和个人的恐怖活动。传统恐怖活动主要是指对袭击目标实施暗杀、爆炸、武装袭击、绑架与劫持人质、劫持交通工具、一般施毒及其他传统形式的违法或刑事犯罪性质的暴力、暴力威胁或暴力破坏活动。非传统恐怖活动主要是指新型恐怖活动,即利用现代高新技术手段的恐怖活动和超级恐怖活动。

(一) 传统恐怖活动

传统恐怖活动通常是以炸弹袭击、挟持人质与绑架、胁迫与威胁、虚假信息 and 宣传活动(“神经战”)等传统战术为手段。其中,绑架、袭击和暗杀是恐怖分子常用的手段。这些手段会带来更大的或更持久的社会公众负面效应。

1. 炸弹袭击

此类恐怖活动较为普遍,且能以最小的危险制造最大的社会破坏效应,尤其是那些使用爆炸装置的活动。爆炸通常能制造很大的社会破坏效应,且被选择的目标一般都具有象征性,如使馆、旅游景点、商厦、娱乐场所等易被人们忽视的有影响的场所。此外,威胁、骚扰和暴力是恐怖分子制造紧张气氛的手段。他们有时会在诸如商场、电影院等公共场所安放小型炸弹或燃烧装置。如埃及的反政府恐怖分子曾袭击过参观金字塔和其他景点的旅游团。

炸弹袭击可以匿名进行,而且爆炸也能吸引媒体的注意。虽然由于调查技术的进步以及跨国情报合作的发展,一些爆炸案很快就会被侦破并对恐怖分子进行审讯,如俄克拉荷马城爆炸案和纽约的世界贸易中心爆炸案,但是媒体对爆炸案仍然十分关注。炸弹袭击的类型主要有以下几种:

(1) 针对个人的袭击。此类袭击既包括以个人为目标的攻击,也包括在有可能造成重大人员伤亡的人口稠密地区安置爆炸装置,恐怖分子使用邮包炸弹对付个人,或用简易爆炸装置引爆载满爆炸物的汽车。有时为了确保炸弹能够引爆,司机会采用自杀式袭击。

(2) 对象征性目标的袭击。一般是各级政府机关、重要(政治、经济、军事)目标设施、有影响企业的设施或历史性标志。这类袭击通常选择在特定的时间和地点。

(3) 选择性目标袭击。恐怖分子为了某种信念或意识形态,可能把目标对准特定的设施和人群。他们的袭击可能针对政府和政府的某个机构,或某个私人企业的建筑、财产或人员。

(4) 持续的炸弹袭击。这类袭击是要吸引人们对特定目标的注意力,比如释放在狱中的犯罪集团成员或恐怖组织同伙。这类组织的典型案有“真正爱尔兰共和军”对英国目标的系列袭击,以及本·拉登对美国目标的袭击等。

2. 挟持人质与绑架

恐怖分子可能采用挟持人质、大规模挟持人质或者其他与人质有关的方法来胁迫政府或私营企业,让其按某种方式行事、终止某项行动,或修改某个决定或决策。恐怖分子作案时如果遇到警察的拦截,他们可能会利用人质来帮助自己逃脱。挟持人质和绑架两者之间有区别。在挟持人质事件中,人质被扣押的地点是已知的,绑架则不然。绑架事件还常常伴随索取赎金,以为恐怖组织提供资金。

3. 胁迫与威胁

恐怖分子单纯使用威胁手段本身就是一种武器。这些威胁有很多种不同的形式:

(1) 用炸弹威胁。这仍是最有效的一种威胁、胁迫工具。除了威胁特定目标如学校之外,这种方法对私人拥有的设施和工业设备也特别有效。

(2) 进行欺骗或恶作剧炸弹袭击。利用模仿的或者简易的爆炸装置可能比使用匿名威胁造成更长时间的恐慌。

(3) 利用环境或公共服务进行威胁。这种方式可以在短期内产生广泛的混乱和不安。近年来,由于东京地铁系统发生了沙林毒气事件,用生物或化学手段进行袭击或威胁的可能性正逐渐增加。这种威胁还包括污染公共水源、在大众运输系统制造混乱等。

(4) 进行抢劫和敲诈。包括从武力抢劫到强制收取保护费等一系列活动,其目的是筹措资金,供恐怖组织和恐怖活动使用,包括采购武器,租用和维护藏身处,获得运输工具,进行高级训练,维持日常开支等。

(5) 进行其他犯罪活动。包括所有为恐怖组织筹措资金或推进恐怖组织目标的活动。贩毒是恐怖组织的一种主要收入来源,几乎所有的恐怖组织都以某种方式卷入毒品活动,要么是直接贩毒,要么是为毒贩提供安全或其他服务。

(6) 实施破坏和颠覆活动。破坏活动是故意破坏财物,或者是用爆炸以外的办法给工业或政府运行制造混乱。这种行动包括闯入或非法进入特定地点,骚扰或恐吓对方,或干脆占

领该地点。另外,还有破坏电力传输线路和石油运输管道、各种方式的纵火及其他各种破坏活动等。颠覆活动包括封锁军事设施并毁坏财产,在街头示威中打、砸、抢,煽动公民破坏运输设施或扰乱国家机关工作秩序,或其他打着“抗议”旗号进行的活动。这些活动起初往往都是在恐怖组织的支持下开始的,并且成为表达愤怒和抗议的一种方式。

4. 虚假信息和宣传活动

恐怖组织(分子)经常把虚假信息、宣传活动和操纵媒体作为一种恐怖活动的战术手段。这些恐怖活动包括:用电话或信件宣传政府和警察的错误、散布谣言或发布恐吓信息制造恐怖气氛,并且尽可能地利用政府所有的腐败、错误之处扰乱社会秩序,达到其施恐的社会目的。

5. 暗杀

暗杀已经被证明是对各类社会团体和个人目标最为有效的一种普遍的威吓手段。

(二) 新型恐怖活动

新型恐怖活动是相对于传统恐怖活动而言,指恐怖分子采用新技术手段在新领域与人类为敌的恐怖活动,诸如信息恐怖、生态恐怖、金融恐怖、贸易恐怖、文化恐怖、经济恐怖、激光恐怖、基因恐怖等。

1. 利用信息技术实施恐怖活动

利用信息技术实施恐怖活动,是指在信息的获取、传递、处理和运用等实施过程中,运用信息技术(传感技术、通信技术、计算机技术、大数据物联网等)对计算机网络中的信息系统进行破坏与摧毁的恐怖活动。

在信息恐怖活动中,恐怖分子常运用计算机网络等技术手段,利用、削弱、破坏和摧毁对方计算机网络系统的效能,同时保持己方计算机网络系统正常工作,以网络攻击等手段达到削弱、破坏和摧毁对方计算机网络系统的目的;运用电子技术手段和电子干扰设备,破坏对方网络的物质基础,干扰、破坏、瘫痪对方网络中的通信设备,如电缆、光缆、微波站点、电子设备、计算机终端、网络节点、通信卫星等,使对方的通信联络中断,电子设备失灵、计算机停止工作、网络节点断开。恐怖分子(或组织)还可以通过电磁干扰技术、电磁脉冲干扰技术、微波干扰技术、粒子束干扰技术,对对方网络或网络中的任一节点展开主动信息打击。可以采用计算机病毒、高能电磁脉冲、微型纳米机器人、网络嗅探器以及黑客技术进行信息攻击等。

信息恐怖活动通常与计算机网络恐怖活动联系在一起。恐怖分子实施信息恐怖活动是依靠信息干扰技术、计算机病毒技术、黑客攻击技术的支持,通过计算机网络,运用拦路抢劫、堆积邮件、以假充真等多种手段,截获对方的机密信息,或删除文件和数据,或破坏摧毁信息资源,或非法获得对方的网络密码和登录口令,然后冒充对方指挥控制机构,随意调用、破坏信息资源。尤其是黑客们常常假冒敌方指挥控制机构,发布作战命令调动敌方的军队和武器装备进入预设的作战地域,从而达到导致敌方作战失败的目的。

电磁恐怖活动,也是一种信息恐怖活动,即利用电磁脉冲干扰技术(或电磁装置)进行的恐怖活动。电磁脉冲干扰技术是用功率超过1吉瓦(1吉瓦=1千兆瓦)的电子束发生器触发产生强电磁脉冲,去干扰对方网络信息系统。强电磁脉冲能够使对方网络中心的电子信息设备(如通信、导航、数据处理和计算机系统等)在瞬间遭到严重破坏而完全失灵。

2. 利用生态实施恐怖活动

即运用现代技术对河流、海洋、地壳、极地冰川、大气环流和臭氧层的自然状态施加影响,通过改变降水、气温、大气成分、海平面高度、日照及引起地震等办法破坏地球物理环境或造成区域生态灾害等的恐怖活动,如制造台风、海啸、地震等。为求得尽可能快的发展速度,全球生态环境经常处于突变的临界点上,任何微小变量的加减,都足以引起一场生态浩劫。这正是利用生态实施恐怖活动的现实危害所在。

3. 利用金融实施恐怖活动

即运用金融手段进行的恐怖活动。金融恐怖主义是近年来出现的,这种恐怖活动利用金融渠道进行策划和实施,以破坏金融市场稳定和损害国家经济利益为主要目的。随着全球化的加速和金融市场的快速发展,金融恐怖活动的风险不断增加。因此,如何防范金融恐怖活动的风险备受关注。金融机构是金融恐怖活动的重点攻击目标,如银行、证券公司、保险公司等。恐怖分子攻击的目的之一就是造成金融市场的崩溃或大规模恐慌。

4. 利用贸易实施恐怖活动

即运用贸易手段进行的恐怖活动。如今,“贸易战”已经成了许多国家手中的非军事性战争的工具,致使全世界自由贸易、经济全球化、多边贸易体制和全球产业链遭到重创。国内贸易法的国际化运用,关税壁垒的任意建立与打破,信手拈来的贸易制裁,关键性技术的封锁,特别是最惠国待遇等手段产生的破坏性效果都不亚于一次军事活动。

5. 利用文化实施恐怖活动

即恐怖主义与文明冲突相结合所产生的恐怖活动,是国际恐怖活动的又一种形式。它强调破坏或威胁破坏有文化内涵的目标,包括宗教文物,旨在引起媒体对其恐怖行为进行最大限度的报道,在全球产生轰动效应,给目标国民众造成巨大的情感、心理冲击,同时使国际社会聚焦于恐怖分子希望列入议事日程的事情。

恐怖分子和恐怖组织都可能制造文化恐怖活动。这类恐怖活动可能是一个国家内部不同群体间争端的一部分(最极端形式的内战),也可能被用来当作从局部有限冲突升级到全面文化冲突的“工具”。许多情况下,冲突中的文化因素会转化为宗教因素。如1989年拉什迪事件;1979年麦加圣寺事件;2001年“9·11”恐怖袭击案;2001年阿富汗巴米扬大佛被毁事件;1992年印度阿约迪亚清真寺被拆毁事件等。

文化恐怖活动具有跨国性、长期性、复杂性等特点,大大增加了预防的难度。

6. 利用经济实施恐怖活动

渗透到经济活动领域的恐怖活动,如爆炸、劫持人质、恐吓或暗杀等暴力性质的,或其他有组织犯罪行为。仅以1995年前9个月为例,莫斯科近郊有69个农场被烧,全国有469位企业家被杀害,另有1500多人成为蓄意谋杀的受害者。

这种恐怖活动带来的后果同样是社会道德败坏、丧失信心、麻痹和社会意志消沉,群众对政权和执法机关不满,削弱社会民主制度,阻碍国家机关正常运行。

7. 利用激光技术实施恐怖活动

即运用激光技术致敌方设备、人员丧失抵抗力的恐怖活动。如袭击一架飞机、破坏一辆坦克,可以用炮弹、导弹,也可以用激光束去毁坏光学设备或使乘员致盲。在战场上,一名伤员比一名阵亡者需要更多的照料。杀伤人员可以削弱敌方的战斗力,让敌方恐慌且丧

失战斗意志。在天幕上用激光束投射一个受难圣徒的影像,就足以震慑那些虔信宗教的士兵。制造这样的武器在技术上已没有什么障碍,只是需要往技术成分中添加一些想象力。

8. 利用基因技术实施恐怖活动

即运用基因技术给对方造成巨大的人员伤亡和心理震慑的恐怖活动。基因技术是高新技术,基因技术为人类提供了很多帮助。尤其在医学中,它对人类的贡献很大。不过基因技术的负面效应也可能被恐怖组织(分子)用作施恐的技术依托,如制造成用于未来生物战的基因武器等。基因武器可以在战时或平时时期,在敌方防不胜防的情况下突然使用,既能给敌方造成巨大的人员伤亡,同时也能制造巨大的威慑和恐怖,以摧垮敌方心理防线,使之自动丧失战斗力。

四、国内外反恐斗争形势分析

近年来,恐怖主义及其破坏活动成为影响世界安全与稳定的一个突出因素,被人们喻为“21世纪的政治瘟疫”和“21世纪的幽灵”。当前,恐怖主义威胁不断升级。新形势下恐怖活动出现一些新的特点与动向,反恐斗争面临新挑战。

(一) 国内反恐斗争形势分析

恐怖主义滋生的土壤不可能在短期内得到铲除,国内外的各种因素决定了恐怖活动的威胁依然严峻。作为一个多民族、多宗教国家,我国一直面临着来自国内外的恐怖主义威胁,反恐维稳的任务仍然复杂、艰巨。随着反恐力度的不断加大,恐怖势力的组织形式、活动方式等也在逐步调整、变化;另外,在全球化浪潮风起云涌、信息化革命迅猛发展的背景下,恐怖活动的策略、形态与手法出现了一些新的动向,我国面临的恐怖威胁来源也在扩大,这给反恐斗争带来新的挑战。这些挑战主要体现在:

1. 从边疆向内地不断渗透

以前,人们认识中国内的恐怖袭击一般都发生在新疆、西藏等边疆地区,然而北京金水桥、昆明火车站等恐怖事件则显示出恐怖袭击已不局限于某些特殊地区,而是逐渐向内地渗透。任何人口稠密、安防可以被突破的地方,都有可能受到袭击。恐怖袭击有转向常态化的趋势,恐怖活动短期之内难以根除,全国范围内反恐压力增大。

2. 恐怖袭击的手段方式趋向多样化

近年来,恐怖主义活动不仅由边疆渗透至内地,袭击对象也由最初的政府机关、公职人员,转向城市公共活动中心、公交运输系统和普通平民。我国对危险品有严格管制措施,因此现在的作案工具手段也由枪支、炸弹扩展到汽车、砍刀等,恐怖分子往往根据能利用到的工具材料就地取材,但杀伤力却依然很大。同时,恐怖组织也逐渐吸收平民参与实施恐怖袭击。这些变化使得恐怖分子在普通人群中更容易藏匿,使恐怖袭击更加隐形和难以防范,大大加强了反恐的难度。

3. 恐怖主义威胁的来源复杂化

包括昆明“3·01”严重暴恐案和“6·7”厦门公交车爆炸案等一系列恶性暴力事件表明,我国反恐工作的打击对象包括暴力恐怖势力、民族分裂势力、宗教极端势力,以及本土反人类反社会的极端暴力分子。前三股势力目前已经形成合流,通过使用毁灭性手段,不断制造危害人民群众的恶性暴力事件,制造恐慌和社会混乱,煽动民族仇恨,从而实现分裂国家、

传播极端主义思想或其他政治目的。同时前三股势力也有可能利用后一种暴力分子,使反恐工作面对更复杂和严峻的形势。

4. 恐怖势力的分散化、松散化趋向使防控难度增大

随着反恐力度加大,恐怖势力为逃避打击,出现了分散化、松散化的趋向,同时恐怖活动的随机化、隐蔽化在增强,从而导致查处打击的难度增大。尤其是近年来“独狼式”暴恐活动趋多。此类恐怖分子不属于某个恐怖组织,不接受外界指令,自己策划、单独行动,行动更加灵活、机动,在作案时间、地点及打击目标等方面具有很大的不确定性;同时,由于不像有组织恐怖活动那样存在成员之间的联络、沟通,犯罪的线索和迹象更难发现,很难加以有效的防范和打击。

5. 恐怖活动的国际化与跨境流动刺激我国恐怖主义威胁升级

全球化在促进经济繁荣、社会发展的同时,也为恐怖主义的蔓延带来便利。近年来,一些国内暴恐活动明显受到国外恐怖势力的操控。一些国内恐怖分子出境接受训练、参加“圣战”,有的在境外受训或参加恐怖活动后又潜回国内,继续兴风作浪。还有不少恐怖组织利用跨境金融网络进行恐怖主义融资,为恐怖活动做物质准备。我国的恐怖势力在境外势力的背后支持下借机煽动族群对立分裂,制造民族矛盾,搅乱我国正常和平的发展局面。在境外的某些组织势力受到国际第三方资助,对某些企图分裂中国的势力一直给予支持。这些因素构成了中国受恐怖主义威胁升级的复杂的国际环境,也增大了我国反恐工作的难度。

6. 信息技术的发展催生网络恐怖主义

随着信息网络的迅速发展,信息传播速度和覆盖面在现代社会都得到了长足发展。网络在造福人类的同时,也被恐怖主义加以利用,“网络恐怖主义”的威胁正日益加剧。恐怖组织利用网络发动黑客攻击,干扰、破坏重要信息系统,制造社会混乱;利用网络宣传造势、传播恐怖思想、招募人员、筹集资金、传授恐怖活动技能,甚至利用网络发号施令,发动恐怖袭击。在我国,恐怖势力也把网络作为实施恐怖活动的重要手段和平台。如“东突”组织利用网站论坛、QQ群、博客、聊天室等平台宣传极端思想、分裂思想;还利用网络发展成员、策划恐怖活动、传播“圣战”视频和制爆技术。恐怖分子在各地流窜、策划联络等也更加容易;恐怖袭击事件的影响力也随之提高,造成的恐慌和负面效益也会波及更加广泛的人群。

反恐工作关系党和国家工作大局,关系国家安全和社会稳定。当前,面对错综复杂的国际国内形势,必须充分认识反恐斗争的尖锐性、复杂性、长期性,应当从国家安全整体战略的高度去看待和把握反恐问题,应当在理性认识恐怖主义成因、现状及趋向的基础上,用系统思维和辩证思维来思考和设计反恐对策,全面提升反恐斗争的能力水平,切实保障人民群众生命财产安全,全力维护国家安全和社会稳定。

(二) 国际反恐斗争形势分析

自“9·11”恐怖主义系列袭击事件发生以来,各国恐怖势力遭到沉重打击,国际反恐斗争取得积极成效,反恐合作共识持续扩大,国际反恐合作成为全球治理和各国互动的重要议题,取得重要进展。与此同时,在全球化的进程中,恐怖主义仍对各国构成现实威胁,国际反恐斗争面临新的挑战,呈现新的特点。

(1)“基地”组织、“伊斯兰国”仍活跃在阿富汗、叙利亚、伊拉克等地,一些恐怖组织加速向非洲、东南亚等地渗透。

从表象上看,美国领导的打击“伊斯兰国”军事联盟、俄罗斯和叙利亚政府军分别在伊拉克和叙利亚战场取得重要战果。“伊斯兰国”恐怖主义势力在两国的根据地缩小,主要控制城市相继丧失,兵源、财源陷入窘境。然而,被逼到墙角的“伊斯兰国”转而加快向域外发展的步伐,在美欧亚和非洲多国接连制造多起恐怖事件。暴恐能量连续释放,并表现出一些新的特征。

(2) 恐怖势力利用高新技术散播暴恐思想、募集资金与人员、遥控暴恐活动,加紧组建恐怖网络。

恐怖组织利用当今世界全球化、信息化的发展,不断传播暴力极端思想和制暴技术。近年来侦破的案件显示,恐怖分子利用网络进行勾连,从而迅速组织恐怖袭击活动。网络快速、即时、广泛的优势使得恐怖效应进一步放大,使得恐怖势力的危害进一步加强。恐怖活动更加隐蔽多样,随意性、突发性更加突出。大批恐怖分子流窜世界各地,全球各地恐怖活动频度、热度上升。

(3) 各国针对反恐合作与铲除恐怖主义土壤采取了系列措施,但成效不明显。

成效不明显的主要原因有两个方面:一方面,发达国家与发展中国家反恐战略互相矛盾。各国利益冲突埋下了大国反恐合作必生龃龉的隐患。恐怖分子擅长利用发展中国家和发达国家的弱点以资助、组织、装备和训练其招募的人员,发动袭击和躲避逮捕。经济落后、资源有限、反恐能力不足导致许多国家尤其是发展中国家无法充分履行反恐义务。对于发展中国家而言,更多注重着力发展经济、改善民生状况、实现可持续发展,这当然与防范和打击恐怖主义的目的是一致的,但其实力与能力都有限,亟须支持与帮助;发达国家在反恐中“只扫自家门前雪”,不愿向发展中国家提供符合其实际需求的反恐援助,也不愿投入过多资源帮发展中国家实现经济发展和减贫脱贫,更不愿看到其与自己“平起平坐”。发达国家与发展中国家在反恐战略上的这种矛盾短期不易解决,国际反恐难以真正形成广泛的统一战线。

另一方面,西方国家的反恐思想具有浓厚的功利主义色彩。基于国家利益的考量,各国对恐怖主义的根源认知不同,关于恐怖主义的定义至今尚无公论。个别国家打着反恐旗号,推行双重标准,奉行单边主义和霸凌行径,炮制所谓人权人道问题,干涉他国内政,干扰国际反恐合作进程。这种在反恐中持工具主义、功利主义的错误做法不仅没有消除恐怖主义滋长的土壤,反倒在一些重大的国际事务中给这些土壤不断“施养添肥”,致使国际反恐难逃“越反越恐”的怪圈。

(4) 恐怖活动手段更加多样。

与传统恐怖活动不同,近年来恐怖活动的实施者组织化程度明显减弱,恐怖势力加大输入极端思想和施暴手段,导致实施恐怖活动的主体为三人以下甚至一人的“独狼”恐怖活动明显增多。袭击对象从军政部门等“硬目标”,向集会人群、交通设施等防范薄弱的“软目标”转移。恐袭方式从炸弹袭击、枪杀和绑架人质等手段向持刀砍杀、驾车碾杀等简单化、低成本化转变,恐怖分子用一把刀、一杆枪、一辆车甚至一个改装的高压锅都能实施恐袭。

(5) 恐怖活动的“烈度”仍未降低,恐怖事件造成大量人员伤亡和财产损失,单次事件伤亡人数巨大的恐怖袭击事件频发。

众所周知,制造恐怖效应是恐怖主义追求的目标。因此,在策划和实施恐怖活动过程中,恐怖组织和恐怖分子会在现有条件下追求最大的伤亡数量以达到制造恐怖效应的目的。

随着恐怖活动的升级演变,各国防范恐怖袭击的措施也不断升级。客观讲,制造大规模杀伤效果的恐怖活动难度也在升级。在世界政治格局动荡的大背景下,意识形态冲突推动下的极端仇恨使得恐怖分子的对抗、报复和挑战也在升级,造成大规模人员伤亡的恐怖事件时有发生。

当前国际恐怖主义形势仍然十分严峻,这给国际社会带来巨大压力,国际反恐斗争任重而道远。

五、交通运输行业反恐防范工作概况

近年来,全球范围内的恐怖袭击事件频繁发生,严重威胁到人民群众的生命财产安全和社会公共安全。交通运输行业具有人员密集流动、公共开放、点多线长面广等显著特点,是国家反恐防范工作的重点行业之一。

(一) 交通运输行业反恐防范工作现状

交通运输行业反恐防范工作面临着很大的难度和工作量。

首先,由于交通运输行业点多、线长、面广、公共开放、人员密集流动等显著特点,其反恐防范工作需要覆盖多种交通方式、多个环节,工作范围广泛,任务繁重。这使得交通运输企业经营部门及公共交通设施管理部门需要投入大量的人力、物力和财力来应对日益增加的威胁。

其次,交通运输行业反恐防范工作面临着恐怖威胁的复杂性和多变性,要求及时、准确地获取恐怖威胁情报,采取针对性的防范措施。这就要建立健全的情报收集、分析和分享机制,以提高反恐防范工作的效果。

再次,交通运输行业反恐防范工作需要充分考虑人防、物防和技防的有机结合。人防方面,相关部门应加强人员培训,提高员工的安全意识和应急处理能力。物防方面,应采取物理隔离、设备监控和安全检查等措施,以阻止恐怖袭击事件的发生。技防方面,可以利用现代科技手段,如视频监控、智能识别等,提升反恐防范的能力。综合使用各种手段,确保反恐防范工作的有效性和实效性。

(二) 交通运输行业反恐防范等级管理

为了提高交通运输行业的反恐防范工作水平,我国建立了反恐防范长效管理机制,以保护人民群众的生命财产安全,保障社会公共安全,并为反恐防范监督检查工作提供依据。地方交通运输主管部门针对本地区的公路水路交通运输系统,组织开展恐怖威胁风险评估,并制订相应的反恐防范等级工作方案。

反恐防范等级由恐怖威胁发生的可能性与潜在后果的严重性两方面决定,综合考虑如下因素:

①反恐防范目标可能遭受的恐怖威胁类型;②所处时段的敏感性和重要性(如举办重大活动期间、召开重要会议期间、春运期间等),或所获取恐怖威胁情报的可信性、明确性和迫近性;③恐怖威胁的潜在后果及其可能造成的影响程度,如人员伤亡、经济损失、环境污染、政治影响、社会影响、国防影响等。

反恐防范等级的确定方法如下:

①恐怖威胁发生的可能性分为低、中、高三个等级;②恐怖威胁潜在后果的严重性分为一般、严重、特别严重三个等级;③采用风险矩阵方法,反恐防范等级由低到高依次划分为一级(日常状态)、二级(戒备状态)和三级(紧急状态)。

国务院交通运输主管部门确定并下达全国或某一地区交通运输系统的反恐防范等级,各省级、市级交通运输主管部门确定本地区的反恐防范等级,省级、市级交通运输主管部门确定的等级不应低于上级主管部门确定的反恐防范等级。

各级交通运输主管部门在发布反恐防范等级变更指令时,应告知交通运输企业经营人及公共交通设施管理人恐怖威胁相关信息、等级起始时间、可能影响范围及其他警示事项。

交通运输企业经营人及公共交通设施管理人在接到反恐防范等级变更指令时,应按照反恐防范等级工作的要求以及指定的反恐防范等级工作方案,及时调整人防、物防和技防措施,同时执行各级交通运输主管部门与反恐部门的指令。

(三) 交通运输行业反恐防范等级工作要求

反恐防范等级工作要求由低到高依次为一级防范要求、二级防范要求和三级防范要求,具体说明如下:

(1)一级防范要求为日常状态下,应当始终保持的基本性人防、物防和技防措施;

(2)二级防范要求为戒备状态下,在落实一级防范要求基础上所采取的附加性人防、物防和技防措施;

(3)三级防范要求为紧急状态下,在落实一级、二级防范要求的基础上所采取的特殊性人防、物防和技防措施。

交通运输企业经营人及公共交通设施管理人应遵从“人防、物防、技防有机结合”的原则,综合有效地运用人防、物防和技防手段。新建、改建、扩建交通运输建设项目的反恐防范设备设施,应与主体工程同时设计、同时施工、同时投入生产和使用。交通运输企业经营人及公共交通设施管理人应不断适应反恐防范工作的新情况、新要求,在各级交通运输主管部门和反恐部门的指导下积极引进先进的反恐防范理念、方法和手段。地方交通运输主管部门应监督检查交通运输企业经营人及公共交通设施管理人在不同等级下人防、物防和技防措施的执行与落实情况。

(四) 交通运输行业反恐应急管理

交通运输行业作为现代社会基础设施的重要组成部分,不仅关系到人民群众的日常生活和经济发展,而且也承担着防范恐怖袭击的责任。恐怖分子利用交通工具进行恐怖袭击已成为一种常见手段,因此,交通运输行业反恐应急管理显得尤为重要。

1. 反恐应急管理的重要性

(1)保障公众安全。交通运输行业直接关系到公众的生命安全和财产安全。恐怖袭击往往导致人员伤亡、设施破坏和社会恐慌等后果,严重威胁着公众的安全感和福祉。通过加强交通运输系统反恐应急管理,可以预防和应对恐怖袭击事件,有效保障公众的安全。

(2)维护社会稳定。恐怖袭击不仅对受害者造成直接伤害,还会引发广泛的社会恐慌和不安情绪,对社会稳定造成严重影响。交通运输行业作为连接城市和地区的纽带,一旦发生恐怖袭击事件,将直接影响公众的日常生活和经济活动。通过加强交通运输系统反恐应急

管理,可以有效稳定社会秩序,维护社会稳定。

(3)保护国家安全。交通运输行业的安全关系到国家的整体安全。恐怖袭击不仅对公众安全构成威胁,也会对国家形象和国际地位造成负面影响。恐怖分子可能利用交通工具进行大规模袭击,破坏基础设施,妨碍国家的经济发展和社会进步。通过加强交通运输系统反恐应急管理,可以更好地防范恐怖主义活动,保护国家安全。

(4)经济发展的保障。交通运输行业对于经济的发展至关重要。一旦发生恐怖袭击事件,将直接影响交通运输系统的正常运行,导致交通瘫痪、物流中断等后果,给经济带来巨大损失。通过加强交通运输系统反恐应急管理,可以减少恐怖袭击对交通运输系统的影响,保障经济的持续发展。

2. 反恐应急管理的挑战

(1)复杂多样的恐怖威胁。恐怖主义手段日趋复杂多样化,恐怖分子可能利用各种手段进行袭击,如炸弹、枪击、劫持等。这对交通运输行业提出了更高的安全要求,为应对不同类型的威胁,各级交通运输主管部门应设立反恐应急领导机构,建立反恐应急处置咨询专家组,制定交通运输系统反恐应急预案,并组织开展演习。

(2)庞大的交通网络。交通运输行业包括陆路、水路、航空、铁路等各种交通方式和设施,庞大的交通网络使得安全管理工作变得复杂而困难。这就需要统筹考虑整个交通网络的安全,有效监控和管理各个环节和节点,防止恐怖袭击的发生。

(3)国际合作与信息共享。恐怖主义是跨国性的威胁,需要加强国际合作与信息共享。交通运输行业需要与其他国家和地区进行紧密合作,分享情报、经验和技術,共同应对恐怖袭击的挑战。同时,也需要建立健全的国内信息共享机制,提高反恐应急管理的效能。

(4)人员培训与专业素养。交通运输行业的反恐应急管理需要专业的人员进行指导和执行。需要加强人员培训,提高相关从业人员的反恐意识和应急处置能力,确保能够迅速、有效地应对恐怖袭击事件。

3. 反恐应急管理的解决方案

(1)建立健全的安保管控体系。交通设施管理部门应制定相应的法律法规和标准,明确各方责任,并建立安全管理机构,加强对交通运输行业的监管和指导。

(2)加强反恐应急人员培训和技能提升。交通运输企业经营人及公共交通设施管理人应开展有效的反恐应急宣传、培训活动,使各级领导、应急管理和救援人员熟悉各自的应急职责、应急响应与处置程序要点。交通运输企业经营人及公共交通设施管理人应定期或不定期地组织本单位反恐应急处置训练,并参加各级交通运输主管部门和反恐部门组织的反恐演习,保证应急预案的有效实施和完善,提高应急反应能力和实战能力。

(3)加强信息共享和联动机制。建立跨部门、跨地区的信息共享和联动机制,加强情报分析和预警,及时掌握恐怖主义活动的动态。

(4)配备更多基础性的技术防控设备器材,提高视频监控技术。

练习题

(一) 判断题

() 1. 目前,恐怖主义在全球范围内已有统一的定义。

()2. 交通运输行业反恐需要提高相关从业人员的反恐意识和应急处置能力。

(二) 单项选择题

1. 以下属于新型恐怖活动手段的是()。
 - A. “神经战”(虚假信息 and 宣传活动)
 - B. 挟持人质
 - C. 生态恐怖
 - D. 武装袭击
2. 恐怖主义的特征不包括()。
 - A. 恐怖主义的暴力具有隐蔽性、突发性
 - B. 恐怖行为会对财产造成危害
 - C. 恐怖主义的打击目标是各国政府、公众或个人
 - D. 所有破坏安全的行为都是恐怖主义

(三) 多项选择题

1. 关于新形势下我国反恐斗争面临的全新挑战,以下表述错误的是()。
 - A. 从内地向边疆不断渗透
 - B. 恐怖袭击的手段方式趋向单一性
 - C. 恐怖主义威胁的来源单一化
 - D. 恐怖势力的分散化、松散化趋向使防控难度增大
2. 以下各项不属于传统恐怖活动类型的是()。
 - A. 炸弹袭击
 - B. 挟持人质与绑架
 - C. 利用信息实施恐怖活动
 - D. 利用生态实施恐怖活动

模块二 港口设施保安概述

一、港口设施保安履约概述

海运是全球重要的贸易运输方式。因运输商品的种类广泛、性价比较高、运输网络遍布等优点,一直以来,海运量占全球贸易运输量的90%以上。长期以来,不法分子不时利用国际航运从事走私、贩毒、偷渡等违法活动。“9·11”恐怖袭击发生后,为有效防范全球港口和船舶受恐怖活动威胁,国际海事组织在讨论了国际海上运输业保安方面的薄弱性后,对《1974年国际海上人命安全公约》(International Convention for the Safety of Life at Sea 1974,简称 SOLAS 公约)进行了重要的修正和补充,并出台了《国际船舶和港口设施保安规则》(International Ship and Port Facility Security Code,简称 ISPS 规则)。国际海事组织(International Maritime Organization,简称 IMO)于2002年12月12日召开外交大会,通过了 SOLAS 公约修正案和 ISPS 规则,修正案和规则于2004年7月1日起生效。

我国于1973年恢复了在IMO中的成员国地位,并从1989年起连续担任该组织的A类理事国。作为航运大国,我国批准或加入了该组织几乎所有重要的公约,并积极参与了SOLAS公约修正案和ISPS规则的制定工作,作为公约的缔约国,中国政府负有全面履行公约的义务。

SOLAS公约修正案出台后,得到了国际社会的积极反应。各国普遍认为,当今世界形势的发展客观上需要一个新的、全面的国际海上保安制度,国际性的问题需要国际性的解决方案。而SOLAS公约修正案把海上保安视为“风险管理活动”,强调了最大限度的统一行动和积极预防的重要性,并为确定威胁、评估薄弱环节提供了操作指导,为保安评估提供了“工具箱”。

二、国际港口设施保安工作概况

(一) 各国际组织不断推进港口设施保安的相关工作

1. 国际海事组织(IMO)

“9·11”事件发生前,有关海上安全和恐怖主义的国际公约主要是《防止危害海上航行的不法行为公约》(即1992年由IMO通过的SUA公约)。对IMO而言,公约的主要目的为“保证对犯有危害船舶不法行为的人员采取合适的行动”。不法行为包括“暴力扣押船舶;对船上人员采取暴力行为;在船上安置可能毁灭或破坏船舶的设备”。保护船舶、船员以及乘客是保证海上和港口安全的重要组成部分,也是SUA公约的目标。但是,该公约没有直接涉及保护港口、岸边设施及人员的安全和保安问题。

“9·11”事件发生后,国际恐怖主义活动日益频繁,港口及海事安全和保安问题被广泛关注。在美国等发达资本主义国家的积极推动下,IMO海上安全国际工作组提出了有关国际海上安全另外措施的建议,并采取了一系列行动。

(1) 相关国际公约的制定与修订。

IMO以前所未有的速度通过了SOLAS修正案。该修正案增加了第XI-2章“加强海上保安的特别措施”。同时为了与SOLAS公约修正案相配套,制定了ISPS规则。ISPS规则包括A、B两个部分,其中A部分是强制性的要求,B部分是对A部分要求的实施提供指导,两者相互对应。

ISPS规则对港口设施保安做了规定,其主要内容是对港口设施提出了保安要求,即对于港口设施需要采取的保安措施包括人员进入船舶或港口设施、船上或港口设施内的限制区域,货物装卸、船舶物料交付、非随身携带行李的装卸,以及监控船舶和港口设施的保安。与此同时,2003年7月1日生效的SOLAS公约第V章修正案对国际航行的船舶提出了配备船舶自动识别系统(AIS)的要求。SOLAS公约第XI-1章提出了关于“船舶识别号”和“携带连续概要记录(CSR)”的新规定。

ISPS规则关于船舶的规定主要有三方面的内容:第一,对缔约国政府的要求。其中包括:应设定适用的保安级别和批准《船舶保安计划》及其后的修改;审核船舶是否符合SOLAS第XI-2章和ISPS规则的有关规定,并向船舶签发国际船舶保安证书;为船舶规定保安等级并向船舶通报有关保安信息;规定船舶何时应要求签署《保安声明》。第二,对船舶本身的要求。其内容主要包括:船舶保安员、船舶保安计划、公司保安员、确定的船上设备设施情况。

同时还要求船舶:对保安措施要有监测和控制途径;提供监测人员和货物的动态;确保有备用的安全通信设施和途径;携带船舶安全保证书。

ISPS 规则的意义在于为各国保安措施的执行提供了一个标准化框架,以评价恐怖主义行为造成的风险,并使政府、港口和船舶的经营者能够根据威胁的程度,相应地调整保安警戒状态和应急反应措施。

(2)对供应链保安问题进行研讨。

2006年5月10~19日,IMO海上安全委员会(MSC)第81届会议在英国伦敦召开。会议在讨论“加强海上保安的措施”这一重要议题时,将供应链保安列为其中一项重要内容。会议专门成立工作组就上述内容进行了讨论。工作组主要就IMO在供应链保安中的地位、责任和应采取的措施进行了讨论。考虑到供应链涵盖货物从生产到销售的全过程,船舶及港口设施只是其中的一个组成部分,因此很多国家对IMO是否在其中承担主要角色提出异议,认为IMO应更多关注于船舶和港口以及与其他运输方式领域内的相关保安工作。中方代表团发言指出,由于供应链管理缺乏统一的国际国内法律框架,IMO宜进一步加强与世界海关组织(WCO)和联合国其他机构的合作,对现有的国际保安法律法规和措施进行充分的评估,稳步推进供应链保安事务。

经过工作组的讨论,委员会同意暂不就此做出决定,但在现有的IMO便利运输委员会(FAL)船港界面工作组(SPI)中增加关于供应链保安的内容,由其就集装箱和其他封闭货物运输工具的保安、是否修正SOLAS公约和ISPS规则以及如何采取与WCO的标准框架对应措施等方面进行研究并提出建议,向MSC第83次会议和FAL第34次会议报告。

(3)研究开发安全软件。

IMO于2005年建立了全球综合海运信息系统(Global Integrated Shipping Information System,简称GISIS)。该系统来自IMO国际船舶信息数据库和港口国数据控制数据库。该系统目前可用的模块包括:船舶识别;ISPS规则的实施;验证机构;海上人员伤亡和事故;状态评估计划等。目前已完成的模块包括:港口国检查;海盗事故报告;偷渡事故报告;非法移民事故报告;报告点;相关安全要求;港口接载信息;压载水管理;公司和登记船东;油污产品目录等。

每个成员国可以获得GISIS的一个用户名和密码登入该网站。关于成员国海上事故和事件的报告,成员国可以通过该系统获得已经通过的有关事故报告的程序和格式,并通过该系统输入要求上报的事故数据资料,提交IMO秘书处审核。经过核准后,秘书处再将各成员国上报数据资料在GISIS公布,供各成员国随时查询。

(4)不断就保安新问题开展讨论。

MSC第85届会议审议了通信工作组提出的《非SOLAS公约船舶保安导则》(包括客船外的商业性船舶、客船、渔船、游艇等四类船舶和有关港口、码头管理导则)。考虑到该文件的自愿性质,包括我国在内的发言国家总体上支持制订该导则。我国同时建议有关内容简单易行、具有实践可操作性。挪威、瑞典、丹麦、德国、爱尔兰和马耳他等部分国家表示其无法执行其中关于游艇与港口和码头管理等两部分内容,要求予以删除。会议最终在重申该导则以作为将来任何法律行动基础的前提下,以通函形式予以批准。挪威等国就游艇与港口和码头管理等两部分内容做了保留。

2012年,IMO出版了《IMO海上保安和〈ISPS规则〉指南》(简称《指南》)的第一版,以协助成员国政府实施ISPS规则。该《指南》的目标是协助成员国实施IMO的海事安全措施,其中包括SOLAS第XI-2章和ISPS规则、《国际海事公约》中规定的强制性规定。SUA公约以及MSC通过的各种指南。自2012年以来,在IMO的全球海事安全综合技术合作计划(ITCP)下,海上安保与便利部门(MSF)以《指南》为基础,开始实施该计划。

IMO于2017年1月10~12日举行《吉布提行为准则》签署国高级别会议,通过了修订后的《吉布提行为准则》(即《2017年吉布提行为准则吉达修正案》)。修订后的《吉布提行为准则》以2009年在IMO主持下通过的早期准则为基础,呼吁签署国尽最大可能合作,打击海上领域的跨国组织犯罪、海上恐怖主义,以及非法、无管制和未报告(IUU)捕鱼和其他海上非法活动。签署国承诺制定国家海上保安政策和国家立法,以确保港口设施的安全运营以及有效保护海洋环境和可持续管理海洋生物资源。

(5) 实施相关保安活动项目。

目前,IMO海事安全部门正在开展一项新的旨在解决非洲东部和南部及印度洋的港口安全和航行安全问题的活动项目。该项目由欧洲联盟赞助,在印度洋委员会(海委会)总体战略指导下,将与国际刑事警察组织(刑警组织)和联合国毒品和犯罪问题办公室(毒品和犯罪问题办公室)共同实施。受援国包括安哥拉、科摩罗、肯尼亚、马达加斯加、毛里求斯、莫桑比克、纳米比亚、塞舌尔和坦桑尼亚。

该项目的主要目标是:①加强欧洲联盟—非洲联盟—伊斯兰组织区域航运当局的安全能力;②支持制定港口安全立法和相关合规框架;③建立关于货物和乘客的区域信息共享机制和数据交换系统。

IMO将与受援国合作,提出若干关键倡议,以加强各国政府和港口两级的海事安全。其中包括战略要素,如支持发展国家海上安全委员会,支持加强SOLAS第XI-2章和ISPS规则中有关港口保安措施的政府监督能力,开展国家桌面演习,协助编写港口设施保安评估和港口设施保安计划,以及支持规划和开展海上保安演习。这一整套技术援助活动有助于在受援国内部和整个经济区、南美洲和经济一体化组织区域长期持续地改善海上安全。

2. 世界海关组织(WCO)

2002年6月,世界海关组织(World Customs Organization,简称WCO)通过了一项关于国际贸易供应链保安与便利的决议,以便确定实施措施来保护国际贸易免受恐怖分子袭击,确保国际物流链不被恐怖分子用作非法运输大规模杀伤性武器。

2003年6月,WCO理事会通过了一项新的《关务行政互助国际公约》,要求各成员国通过其海关当局,相互提供援助,确保国家贸易供应链的安全。

2005年6月,WCO通过了《全球贸易安全与便利标准框架》(简称《框架》)一揽子文件。其宗旨是制定全球范围供应链安全与便利的标准,促进稳定性和预见性;形成对所有运输方式适用的一体化供应链管理;增强海关应对21世纪挑战和机遇的作用、职能和能力;加强成员海关之间合作,提高甄别高风险货物的能力;加强海关与商界的合作,通过保护国际贸易供应链安全促进货物畅通无阻的流动。

《框架》的内容主要包括了4个核心元素、2个支柱、17项标准和关于这17项标准的技术性条款。4个核心元素包括:①要求提前递交进出口及转运货物的电子信息;②采用一致

的风险管理手段;③应进口国的合理要求,出口国海关对出口的高风险集装箱和货物进行查验;④要求海关要向满足该标准的商界提供相应的便利。基于这4个要素,《框架》提出了保障供应链安全的两大支柱,即海关与海关之间的合作安排和海关与商界之间的伙伴关系。第一个支柱即海关与海关之间的合作安排,包括了“海关应遵照WCO在《综合供应链管理指南》(ISCM Guidelines)方面规定的海关监管程序进行操作”等11项标准,涉及供应链管理、查验权力和查验技术、风险管理和布控、电子信息交换、绩效和安全评估以及工作人员的廉政等海关监管工作的各个方面。这些标准还将鼓励海关和其他政府部门之间的合作,帮助政府实施统一的边境管理和控制,并通过采取必要措施,使政府能够扩大海关在这个领域的权限和职责。第二个支柱即海关与商界的合作,包括6项标准,企业应执行以海关设定的安全标准为参数的自我评估程序、供应链经营者本身应采取的安全措施、授权认证的取得、新技术的采用、与海关的合作与交流以及获取贸易便利的条件,等等。这其中,取得“授权经营人(Authorized Economic Operation,简称AEO)”^①的地位并得到供应链中其他各方的承认,对从事国际贸易的企业来说可能是最重要的,这将使其可以得到各方的信任并得到各项贸易便利措施所带来的好处,比如由于查验率降低而使得货物的通关速度加快,因为建立了一套国际标准,实现了一致性和可预见性,减少多样而复杂的报告要求,从而节约时间和成本等。

为实施这些标准,《框架》还就每项标准制定了详细的实施细则(也称作技术性规定)。比如关于第二个支柱标准的实施细则规定,关于伙伴关系,“共同制定的海关——商界伙伴关系文件应尽可能根据授权经营人商业模式,启动书面的可验证的安全步骤和程序,以保证AEO的商业伙伴,包括生产商、产品供应商和一般的商人宣布遵守保障全球贸易安全与便利标准框架中各标准条款的意向”;关于安全问题,“应通过必要的自动备份方式,诸如需要定期换发新证的个人分配密码账户,适当的信息系统安全培训和对于未授权进入或误用信息的保护来保护贸易敏感数据”;关于授权认证,“海关当局应和商界代表一起设计一套确认体系或者资质鉴定制度,使企业通过获取授权经营人资格而得到激励”“各海关应对授权经营人地位予以互相承认”。《框架》的标准和实施细则,大都来源于世界海关组织已制定的有关公约及其成员的一些比较成功的实践经验。

《框架》提出了海关与海关之间的合作安排和海关与商界之间的伙伴关系,要求其成员国和地区的海关致力于多边而不是双边的反恐统一行动,这可以从根本上铲除恐怖分子对供应链管理的威胁。

此外,世界海关组织未来将以集装箱的安全运输作为防范措施的重点。WCO总干事米希尔·戴尼特(Michel Danet)在《美国托运人》署名文章中指出,经济全球化和贸易自由化,以及交通手段的提高和电子商务的迅猛发展,都对世界海关管理和政策协调提出了新挑战。全世界大部分国家和地区的海关管理当局终于明白,装船前提前递交所谓集装箱舱单信息仅仅是供应链安全总体中的一个环节而已,今后海关当局对供应链的安全监管范围必须扩

^① 授权经营人:在《框架》中被定义为:以任何一种方式参与货物国际流通,并被海关当局认定符合世界海关组织或相应供应链安全标准的一方,包括生产商、进口商、出口商、报关行、承运商、理货人、中间商、口岸和机场、货站经营者、综合经营者、仓储业经营者和分销商。

大,而其真正的重点是远洋集装箱运输。

据统计,仅仅世界供应链管理这一块总共可以产生 4720 亿美元年收益,而且在今后的几年内将以平均每年 500 亿美元的幅度不断增长。集装箱运输是世界供应链中的重要内容。没有集装箱运输业,所谓供应链将名存实亡,正因为如此,全球各个国家和地区都在竞相发展集装箱运输。自从各国海关当局发现集装箱不仅可以载运货物,而且可以藏匿偷渡者、毒品、走私品和其他违规物品,甚至进行恐怖犯罪活动的时候,WCO、各国政府和地区海关当局一致认为,必须通过世界海关组织等国际机构,把全球的反恐力量全部动员起来,才能从根本上确保世界各国港口的安全,尤其是国际集装箱运输的安全。

WCO 集装箱工作小组推出的“供应链安全指导原则”成为由海外国家,尤其是从非集装箱安全倡议(CSI)缔约方的港口出口到美国的集装箱货物提供一条安全“绿色通道”。与美国 CSI 出台过程不同的是,“供应链安全指导原则”在酝酿过程中曾经邀请来自发达国家、发展中国家和不发达国家的承运人、托运人、制造商、经纪人、海关、港口码头经营人的代表,详细听取他们的意见和建议,具体项目包罗万象,甚至涉及集装箱设备和集装箱船舶的发展前途、铅封技术等。但是米希尔·戴尼特总干事同时指出,WCO 是一个不具备约束力的国际组织,其功能和作用仅仅是建议海关当局采取“供应链安全指导原则”,不断提醒组织成员的海关全面执行全球集装箱安全规划的巨大经济利益。

目前,WCO 正在全球推行“海关一体化管理链”工作,要求各个国家和地区的海关当局在最低标准控制操作和风险管理标准上达成多边或双边协议,互相分享情报、信息,通报托运人档案资料和集装箱货物的供应链动态。

3. 国际劳工组织(ILO)

为加强对国际海员的安全保障,ILO 在 2005 年 6 月召开的国际劳工大会上,通过了第 185 号公约,即《2003 年海员身份证件公约》(Convention on Seafarers' Identity Documents)。该公约内容包括海员身份认证制度,制定了全球统一的证件格式和具体技术参数;防伪技术的新成果将应用到海员身份证件中,使海员身份证件的防伪措施能够随着技术的进步而得以改进;引入了海员指纹的生物测定信息,由于使用生物测定技术在海运界是个新事物,大会决议敦促国际劳工局采取措施,与其他组织特别是国际民航组织(ICAO)合作,制定可操作的生物测定国际标准。应该说,新的海员身份证件通过现代技术手段和国际合作,核实在港口、机场和船舶上的海员的身份,将为国际反恐保安做出积极贡献。

此外,ILO 制订了 ILO/IMO 港口保安操作守则,将 ISPS 规则功能性要求扩展至更大范围的港口区域;为政府、雇主、工人和其他利益方之间的有效合作、协调和沟通提供指导。

4. 国际标准化组织(ISO)

国际标准化组织(ISO)认为,国际贸易体系面临的主要挑战之一是对全球供应链的保安威胁,于是在供应链保安领域表现积极,为保护人员、货物、基础设施和设备,制订了一系列文件,出台了最佳实践导则,以预防供应链中可能出现的破坏性影响。ISO 在 2005/2006 年度,将有关供应链保安的文件发布为《公开提供的规范》(PAS)系列之一,包括 ISO 28000、ISO 28001、ISO 28004 和 ISO 28005 全新的 ISO 28000 系列标准为组织机构确立了准则,以识别和管理自然或人为灾祸的相关风险,大幅减少其影响。该系列标准采用了过程方法和“计划—实施—检查—处置”的方法,参与质量、环境或健康与安全管理体系的人员均熟悉该方

法,且有助于独立进行第三方的评估和认证。

(1) ISO 28000。

ISO 的船舶和航运技术委员会(TC8)于2005年底出台了ISO/PAS 28000:2005《供应链保安管理体系规范》,当中汇集了国际海事组织、国际港口和码头协会、国际航运协会、WCO、国际创新贸易网、世界航运委员会和安全技术战略委员会等组织机构的建议。该标准的更新版本ISO/DIS 28000已于2007年发布。ISO/DIS 28000要求组织机构的最高管理层制订安全管理总方针,与组织机构的安全威胁和风险管理整体框架一致,并与组织机构所面临的威胁及其运作的性质和规模相称。此方针必须加以部署和实施,包括安全风险的评估和计划、有效实施和运作、检查和纠正措施及管理评审。

该规范描述了把货物从原产地运输到最终目的地的全过程,包括货物的流动、运送数据、相关的步骤以及一系列动态的关系,它涉及了许多的实体,如货物的生产者、物流经营公司、拼装业者、卡车运输公司、铁路运输公司、航空货物承运人、海运仓库经营者、海运承运人、货运和清关代理人、金融和信息服务部门和被运输货物的买主。

(2) ISO 28001。

ISO在2006年发布了ISO/PAS 28001《供应链安全管理体系——供应链安全的最佳实践规范——评估和计划》,以补充ISO 28000的规定要求,促使组织机构做出更好的风险管理决策。此外,ISO 28001还为独立第三方的审核活动提供选项,以配合和补充世界海关组织的标准框架,保护和促进全球贸易。ISO/PAS 28001是一项供各公司、港口等自愿选择的标准。该标准的要求包括:制订保安计划,确定应对特定威胁的保安措施;明确保安计划所涵盖的供应链范围;开展保安评估,识别供应链存在的保安薄弱环节;制定培训方案,向供应链中的有关人员讲授供应链保安措施。

(3) ISO 28004。

2006年,ISO发布了ISO/PAS 28004《供应链安全管理体系——ISO/PAS 28000实施指南》,旨在协助标准使用者理解和实施ISO 28000,从而获取更大的利益。ISO 28004对ISO/PAS 28000的基本原则进行解说,并描述其目的、特有的输入程序、过程和特有的输出程序。ISO 28004解释了安全管理体系的细节和复杂性、文件记录范围及其需用的资源,均取决于组织机构的规模和复杂性,以及其业务性质。此外,它还明确指出组织机构应有相当的自主权和灵活性,以界定ISO/PAS 28000的实施范围,即整个组织机构、特定运作单位或特定活动。

5. 亚洲太平洋经济合作组织(APEC)

自2006年起推动贸易恢复计划(TRP),旨在通过建立一整套计划、程序和安排,以便在发生恐怖事件后尽快恢复贸易;履行ISPS规则调查问卷,反映ISPS规则在APEC地区履行5年来面临的挑战、不同经济体的差距和共同利益;执行APEC地区港口保安示范访问计划(非强制性,分为“接待访问”和“参加访问”两种,在2008年8月APEC第31次运输工作组会议上,我国以“参加访问”的身份加入该访问项目);向澳大利亚和美国提交了海员身份识别和港口工人身份识别调查问卷,将作为技术支持项目的组成部分列入港口访问项目;制定APEC地区港口设施保安训练、演习手册,在APEC第30次运输工作组会议上通过后,于2008年7月在韩国釜山举行了第一期研讨班,第二期也已于当年秋季在加拿大温哥华举行。

(二)代表国家和地区的港口设施保安工作现状

随着恐怖主义活动的进一步升温,为保证国家利益,各国根据 SOLAS 公约和 ISPS 规则,积极制定了符合本国实际的相关规则,有的采取了更为严格的控制措施,确保供应链安全。至此,货物运输环节的安全与保安问题被进一步扩展。

1. 美国的港口设施保安管理

自“9·11”事件后,美国政府通过制定相关法律和采取专项行动计划等措施,不断强化其港口及航运保安措施,主要包括:

(1) 制定相关法律制度。

自“9·11”事件后,美国政府不断强化港口与海上保安工作,并做了大量的立法工作,提出的影响海上保安和港口安全的议案和法案数量惊人,主要包括:《2001 年港口和海上安全法》《港口威胁和安全法》《2001 年美国安全法》《港口安全和恐怖主义防范法》《2002 年扩大的边界安全和签证人改革法》《2002 年海上运输安全法》《船舶、船员和集装箱安全法》《2002 年海上运输反恐法》《2002 年减少美国海港犯罪和恐怖主义法》《2006 年港口保安及责任法》《2007 年海运货物扫描法》等。这些法案合并了新、旧及新旧交织的想法和观念,既考虑了新技术的发展与应用,又兼顾到传统和成熟的现有技术和设备。这些立法的主要内容和要点体现在建立国家和地方咨询委员会、特别工作组或类似部门、薄弱环节评估、反恐计划、货物安全、雇佣限制与背景调查、身份证明证件、改良海关报告程序、船舶到达前的早期通知、改善船舶跟踪、改进海上安全贷款担保和批准、海上执行官计划等等。

上述法律中,《2001 年港口和海上安全法》(the Port and Maritime Security Act 2001)和《2002 年海上运输反恐法》(Maritime Transportation Anti-terrorism Act of 2002)不仅规定了美国海上反恐制度的框架和原则,而且也构成了美国港口安全制度的核心和基础。其中关于港口安全的内容主要包括:要求美国海岸警卫队对美国港口进行薄弱环节评估;要求海岸警卫队评估那些船舶驶往美国或对美国形成恐怖危险的外国港口所实施的反恐安全措施的有效性;要求那些从外国港口到达美国的商业船舶经营人提供旅客和船员证明,其中包括每个旅客和船员的出生日期、国籍、护照和签证号码及原籍;修改了《港口航道安全法》的规定,要求所有进入美国 12 海里领海的船舶在进入该领域前 96 小时通知海岸警卫队,扩大了海岸警卫队的管辖权;允许派遣海岸警卫队人员在某些设施和船舶上进行侦察并对恐怖活动予以回击。

2002 年,美国修订了《海上运输安全法》(Maritime Transportation Security Act),作为执行 SOLAS 公约和 ISPS 规则的法律依据。该法案于 1996 年通过,是一部旨在提高美国海上运输系统安全性和反恐能力的法律。《海上运输安全法》规定了一系列措施,以确保在美国水域航行的船舶、港口和码头的安全。《海上运输安全法》的主要内容包括以下几个方面:①船舶安全。该法案对船舶的结构、设备、人员培训和操作等方面提出了具体要求。同时,要求船舶定期进行安全检查,确保船舶始终处于良好的运行状态。②港口和码头安全。《海上运输安全法》要求美国境内的港口和码头实施严格的安全措施,包括物理安全、人员安全和网络安全等方面。此法案还要求港口和码头制定应急预案,以应对可能发生的安全事件。③货物运输安全。该法案对货物运输过程中的安全措施提出了具体要求,包括货物装卸、运输和卸载等环节。同时,要求船舶和港口对危险货物进行特殊管理,确保危险货物的安全运输。

④防恐和安全合作。《海上运输安全法》强调了防恐和安全合作的重要性,要求美国与其他国家和地区在海上运输安全方面开展合作,共同应对国际恐怖主义和其他安全威胁。

2003年10月,美国国土安全部在广泛征求各方面意见和建议后,宣布批准和出版最新的《海运业保安规则》(Maritime Industry Security Rules)。该规则主要包括:①保安措施:强化保安;②引导安全评估:确定潜在的易受害环节,并且帮助决定需要实施哪些保安措施;③制定保安计划:对由评估所确定的独特的安全方面事宜允许加以灵活处理;④向海岸警卫队提交计划以获其批准:确保与美国海运业的一致性;⑤确定保安官员:在海运业着重就保安事宜建立保安人员网,同时还提供附加的消息灵通“耳目”;⑥面临增长的威胁而增加保安度:允许在正常的环境下采用更多的中等程序措施,同时确保海运业准备就绪在必要时强化保安;⑦在大型船舶上安装自动识别系统:考虑采用综合全面、实际即时的船舶追踪和监视手段,增强将守法船舶和涉嫌违法船舶区分开来的能力。

在美国,所有海上保安和港口安全立法都涉及一个普遍问题,即要求以发展国家、当地或私人船舶或港口设施为基础的反恐计划。如:《2001年港口和海上安全立法》《2002年海上运输安全法》和《港口保安及责任法》等,都包括了反恐计划的相关规定。

(2) 采取专项海运保安措施。

“9·11”事件后,美国采取的海运反恐措施主要有集装箱安全倡议(Container Security Initiative,简称CSI)、海关—贸易反恐伙伴计划(Customs Trade Partnership Against Terrorism,简称C-TPAT)、海关装船前24小时申报舱单规则(简称“24小时规则”)、商业营运安全计划(Operation Safe Commerce,简称OSC)、《进口商安全申报及对承运人额外要求》管理规定和集装箱全量检查实证实验等,这些措施和规则的实施是为了提高整个供应链的透明度和安全度。

① 集装箱安全倡议(CSI)。

美国集装箱安全倡议是美国全球反恐战略部署的重要组成部分,目的在于防止恐怖组织或恐怖分子利用海运集装箱袭击美国。CSI的主导原则是把甄别货物安全风险和查验的环节前置在海运集装箱的出口港和装运港,使美国的边境或港口由第一道防线变为最后一道防线。CSI的主要内容具体由四方面组成:一是以对预先获得信息的风险目标分析为基础制定高风险集装箱的识别标准;二是在集装箱运往美国之前进行预先甄别;三是运用科学手段预先检查高风险的集装箱;四是设计和使用智能化的安全集装箱。

② 海关-贸易反恐伙伴计划(C-TPAT)。

海关-贸易反恐伙伴计划是美国国土安全部边境保护局(即US Customs and Border Protection,简称CBP)在“9·11”事件发生后倡议成立的与商界一起自发建立的自愿性计划。该计划于2001年11月推出,并于2002年4月16日正式实行。其主旨在于建立CBP、进口商以及它们的供应链之间的伙伴关系,以加强对进入美国货物的安全保证,同时促进贸易流通。

该计划可以通过美国进口业者,要求物流运输业者和国外供货商必须从货物出厂、国际物流运输到美国进口业者的供应链全程有关人员、货物、运输设施、仓库以及文件作业都要符合严密的安全程序管理,以共同确保国际贸易与供应链整体安全之合作机制。

③ 海关装船前24小时申报舱单规则。

2002年10月31日,美国海关根据集装箱安全倡议,提出了有关装船前24小时申报舱

单规则。24小时规则规定,对所有挂靠美国港口的集装箱船舶,美国海关单方面强制要求集装箱班轮运输公司和无船承运人在境外港口装船前24小时,必须向美国海关的“自动舱单系统(AMS)”预先申报有集装箱内所装载货物的舱单资料。从新规定生效60天后的2003年2月1日起,相关承运人在集装箱装船前的24小时,将准确而完整的舱单资料,预先用电子方式传送到美国海关的AMS,否则将面临首次违规罚款5000美元、第二次违规罚款10000美元,以及货物不许在美国港口卸驳的严重后果。

④商业营运安全计划(OSC)。

商业营运安全计划是美国运输部及海关总署所倡议的安全商务行动措施,主要是以提高新的安全性技术测试,增进集装箱运输安全性为主。除了强调海运集装箱的管理和控制外,更广泛地应用于集装箱货物自起点到终点的移动。该计划是CSI及C-TPAT的配套方案。OSC以洛杉矶港/长滩港、纽约港/新泽西港和塔科马港/西雅图港三个主要港口港为试验地。

⑤《进口商安全申报及对承运人额外要求》管理规定。

2008年11月25日,美国海关和边境保护局(CBP)在《联邦公报》(73 FR 71730)上发布了一项题为“进口安全申报和附加承运人要求”(Importer Security Filing and Additional Carrier Requirements)的临时最终规则,要求进口商和承运人在货物通过船舶运抵美国之前向CBP提交与货物有关的额外信息。2009年1月26日,名为“进口安全申报和附加承运人要求”(俗称“10+2”)的新规则生效。该规则主要内容是要求对从其他国家运往美国的货物,美国进口商和船舶运营承运人必须至少在货物装船前24小时前为通过船舶抵达美国的非散装货物运输向CBP提供额外的预先贸易数据,包括提供制造商或供货商的名称和地址、卖方的名称和地址、买方的名称和地址、接受货物方的名称和地址、货物的装箱地、装箱人的名称和地址等。该规则赋予美国国土安全部(DHS)和CBP更大的权力来识别高风险货物,以防止走私并确保货物安全。2010年1月26日,为期12个月的灵活执法期结束,进口安全申报(ISF)正式执行。

根据2009年7月17日的美国海关公告,对于不准确、不完整或不及时的ISF申报,CBP会保留3年的追溯期,针对每项违规行为可能会处以5000美元的罚款,最高可达10000美元。如果货物在没有提交ISF的情况下到达美国边境,CBP有权拒绝卸货,并有权扣押未经授权卸货的货物。

⑥电子自动出口系统。

美国海关总署与美国统计局合作制订和出台了专门用于搜集出口货物资料和运输信息的“电子自动出口系统”。通过这个系统,美国调查局可以精确统计美国的贸易数据,而美国海关总署则可以集中监管高风险集装箱货物。但是这套系统显然已经跟不上当前的反对恐怖主义斗争的需要,因为这套自动出口系统所收到的信息大部分是已经装箱、已经装船,甚至已经抵达卸货港的集装箱货物的信息,对于反恐斗争的实际要求来讲显然为时太晚。

2. 欧盟港口设施保安概况

(1) 从立法角度奠定保安管理基础。

目前在欧盟各成员国范围内,被各国所普遍遵守、涉及港口设施保安的文件除了SOLAS公约修正案和ISPS规则外,主要有两个规定:

①2004年通过的《关于加强船舶和港口设施保安》(725/2004号文件)。