# 第一篇 概述篇

反击信息恐怖活动，确保信息安全，已成为世界各国普遍关注的重大战略课题。本篇用 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。

# 第一章　恐怖活动是威胁人类安全的“政治瘟疫”

随着信息技术的迅猛发展，网络已被广泛应用到国家的政治、经济、军事和人们的日常生活等各个领域，恐怖组织和恐怖分子开始利用信息技术手段在上述领域实施恐怖活动。通过入侵计算机和计算机系统，直接攻击政治、经济、国防、安全等各个要害领域，甚至带来全局性的瘫痪与损失。如恐怖分子在重要计算机供电线路上装上脉冲发生器，发生的脉冲可使计算机存储的数据消失得一干二净。在世界范围内，袭击计算机已占目前恐怖活动总数的一半以上，许多恐怖组织和个人都涉足这一领域，信息和信息系统已成为恐怖组织日益重要的活动舞台。在深入研究信息领域反恐怖之前，本章重点讨论恐怖及恐怖活动有关问题。

## 一、恐怖与恐怖活动

### (一)恐怖活动的内涵

在汉语里，恐怖主要是指一种心态。《辞海》的解释是：恐怖即恐惧、害怕、畏惧。《辞源》解释：恐怖的意思是极度恐惧。《现代汉语词典》解释：“由于生命受到威胁而引起的恐惧。”在英语中，恐怖(terror) 除了有与汉语相同之意即“极度害怕”之外，还包括“恐怖统治”之意。所谓恐怖统治，是

特指法国大革命期间的“雅各宾专政”，意指“无情地处决威胁革命政权之人”。

恐怖活动实际上就是指使人感到极度害怕的行为，或者说是使人感到生命受到威胁的行为。具体地说，恐怖活动是指以任何暴力行为，或威胁从事针对个人、集体、国家的犯罪活动，其目的是以恐怖行为制造恐惧气氛，威胁、伤害或危害他人生命、声誉、自由、人身安全和权力；或威胁破坏任何公共设施及公共、个人财产；或危害国家资源、国家设施；或威胁国家主权和安全、领土完整和国家统一；或威胁有关政府、社会，为达到某种目的服务。例如：无论强者或弱者都可采用的，针对非战斗目标（特别是无辜平民）的暗杀、爆炸、武装袭击、绑架与劫持人质、劫持交通工具、施毒、核袭击、生化袭击；危害计算机系统、实施网络袭击、采用信息战破坏或摧毁信息系统等手段制造的信息恐怖活动，以及其他形式的违法或刑事犯罪性质的暴力、暴力威胁或非暴力破坏活动，均属于恐怖活动的范畴。

(二)恐怖活动的新特点

随着科学技术的发展和人们生活水平的提高，恐怖活动除了具有恐惧性、暴力性、违法性等特点外，还具有许多特殊的新的行为特点，如隐蔽性、任意性、高技术性、组织形式网络化等。

1. 隐蔽性。近年来，恐怖活动的策略已由署名的示威性恐怖活动转向隐蔽性的恐怖活动。即使有的恐怖分子在行动之前公开发出恐吓，但其行为也仍然是隐蔽的，且呈越来越隐蔽的趋势。人们不知道恐怖分子在哪里，可能在哪里采取行动和采取什么行动，其行动的直接目标是什么。这构成了恐怖分子行为的突发性、任意性和难以预防性。

在2001年“'9·11”事件发生之前，美国遭受了一连串据

认为是“恐怖大亨”本·拉登所策划的恐怖主义袭击，这些袭击对美国造成了很大的恐怖影响。2001年6月，美国得到可信情报，本·拉登组织要对美国目标发动大规模袭击，但不知会发生在何时、何地、针对何目标。为防止再度发生像2000年美国“科尔”号军舰被炸那样的事件，美国不得不采取全线的防御态势：6艘美国军舰从美国第五舰队总部所在地巴林驶向外海；2200名正在约旦训练的海军士兵提前结束训练；一项海军陆战队的演习被取消；在海湾地区的20多艘美国军舰不得靠岸；2万多名美国军事人员行动受限；美国“星座”号航空母舰受命驶入波斯湾；红海的一支两栖陆战队及美国设在土耳其南部的吉尔利克空军基地进入高度戒备状态。此外，美国国务院还发出了“全球警告”，要求所有美国海外机构和人员保持高度警惕。然而，尽管美国做出了全面周到的部署，但没料到恐怖分子的袭击方式竟是劫持美国国内的民航客机撞向纽约世贸中心和五角大楼。

2. 任意性。就恐怖分子的袭击目标而言，虽然有时选定的政府官员是国家最高领导人，但在多数时候，恐怖分子的袭击是不分青红皂白的，其伤害对象是任意的。如在“9·11”事件中，尽管纽约世贸中心和五角大楼是恐怖分子事先选定的明确目标，但他们所伤害的人员却是任意的。一些宗教极端主义的恐怖分子把攻击对象看作“异端”和“邪恶社会”,对其成员不加区别地袭击，手段极其残忍。如在阿尔及利亚，伊斯兰极端组织经常对一些乡村搞“大清洗”，使一个村庄一个村庄包括妇孺和老人在内的平民惨遭集体大屠杀。1999年底，俄罗斯连续发生居民楼爆炸事件。2000年，东南亚一些国家也不断发生屠杀村民的恐怖事件。

3. 高技术性。随着高新技术的迅猛发展和新概念武器的出现，恐怖分子施恐手段的技术含量也大大增加。从近年来出

现的新型恐怖活动和超级恐怖活动及其施恐手段与途径看来，恐怖分子主要是以信息技术、电脑“黑客”技术、“克隆”技术和大规模杀伤武器（生物武器、化学武器、核武器）及信息战、贸易战、金融战、生态战、文化战等手段进行破坏和犯罪活动，而这些高新技术手段已成为恐怖分子施恐的重要且行之有效的武器与工具。恐怖组织为了谋求更大的杀伤力和破坏性，制造更大的恐怖效应，千方百计地通过各种途径索取和掌握先进科学技术，索取用于恐怖攻击的新器具、新技术、新材料，更新武器装备，“创新”恐怖攻击的形式和方法。如一些恐怖组织购买导弹及核材料、核技术，通过自己培养与招募高技术人才（如电脑黑客）等途径，使一些高技术人员在一定条件下摇身一变为恐怖分子，实施高技术性的恐怖攻击。

4. 组织网络化。组织网络化是指恐怖组织的组织结构形态与分布状况呈网络形态（社会网络）。随着信息技术的发展，恐怖组织（分子）的组织结构已从等级制结构向信息时代的网络结构变化。从当今更新更活跃的恐怖组织看来，其组织结构主要呈现为非中心的、灵活的网络结构。它们从正式的有组织的、国家支持的等级式结构转向松散的等级较少的网络式组织结构。组织内领导让位于等级减少的非中心化结构，即私人资助、松散网络联系起来的个人或小团体等。此外，信息技术的最新发展促进了恐怖组织的网络化。一些恐怖分子不仅把它作为一种武器，实施信息恐怖，而且还用来帮助协调和支持恐怖活动。近年来，恐怖组织越来越多地通过网络利用信息技术来指挥、管理和协调分散的成员活动，传播恐怖活动信息和侦察技术，进行联络和筹措经费等。这样既可支持本身的网络组织，又使得希望远距离活动的小恐怖组织和个人更有攻击力。

## 二、恐怖活动的类型和手段

恐怖活动的类型繁多，由于人们对恐怖活动概念的理解不同，因而对恐怖活动的分类亦不一样。

从恐怖行为者的性质分，可分为政府行为恐怖活动（也称为国家恐怖活动）和非政府行为恐怖活动。政府行为恐怖活动又可分为对内恐怖活动和对外恐怖活动。

按施恐手段分，可分为传统恐怖活动和非传统恐怖活动。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现代恐怖活动（即利用现代技术手段的恐怖活动），主要包括超级恐怖活动和新恐怖活动。

（一）传统恐怖活动

传统恐怖活动手段主要包括：炸弹攻击、挟持人质、劫机、绑架、暗杀、胁迫和威胁、“神经战”（虚假信息和宣传活动）等传统战术与手段。其中，绑架、袭击和暗杀是恐怖分子越来越喜欢用的手段。这些手段会造成更大的或更持久的公众效应。

1. 炸弹攻击。恐怖活动的原则总是以最小的危险制造最大的公众效应，尤其是那些使用爆炸装置的活动。爆炸通常能制造很大的公众效应，这取决于时间和地点，所以被选择的目标一般都具有象征性。例如，使馆、国际知名的旅游景点或类似的地方。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。最近几年，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。炸弹攻击可以匿名进行，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，俄克拉荷马城爆炸案和纽约的世界贸易中心爆炸案很快就被侦破，并进行审讯，但是媒体对爆炸案仍然十分关注。

炸弹攻击的类型主要有四种：

(1) 针对个人的攻击。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(IED) 恐怖分子使用邮包炸弹对付个人，或用简易爆炸装置对准战略目标。恐怖分子所使用的可能是一个炸弹，或者是一辆装满爆炸物的汽车，有时为了确保炸弹能够引爆，司机本人就准备在爆炸中自杀。

(2) 象征性目标的攻击。一般是政府建筑、军事设施、经过挑选的公司企业的设施或历史标志。这类攻击通常选择在特定的时间和地点。

(3) 选择性目标攻击。恐怖分子为了某种信念或政治意识形态，可能把目标对准特定的设施和人群。他们的攻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) 持续的炸弹攻击。这类攻击是要吸引人们对特定目标或事业的注意力，比如释放在狱中的犯罪集团或恐怖组织同伙。这类组织的典型案例包括“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。

2. 挟持人质与绑架。恐怖分子可能运用挟持人质、大规模挟持人质或者其他与人质有关的行动来胁迫政府或私营企业，让其按某种方式行事，终止某行动，或修改某个决定或问题。恐怖分子作案时如果遇到警察的拦截，他们可能会运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知道的，绑架则不然。绑架

行动还常常通过索取赎金来为恐怖组织获取资金。

3. 胁迫与威胁。恐怖分子单纯使用威胁手段本身就是一种潜在的武器。这些威胁有很多种不同的形式。

(1)炸弹威胁。这仍是最有效的一种威胁、胁迫的工具。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)欺骗或恶作剧炸弹攻击。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混乱。

(3)环境或公共服务威胁。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攻击的威胁正逐渐增大。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)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)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。卷入贩毒活动的有名的恐怖组织包括哥伦比亚的“解放力量”(FARC)，斯里兰卡的泰米尔猛虎组织，还有在中东、东亚以及非洲部分地区贩毒的本·拉登。

(6)破坏和颠覆活动。在发生之初可能不会被立即当作恐怖活动。这些活动包括封锁军事设施并毁坏财产，在街头示威中打、砸、抢，通过公民不服从来破坏运输系统或政府运作，或其他在“抗议”的旗帜下进行的活动。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方

式。

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作制造混乱。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。还包括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。

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战术。卡洛斯在他的游击战策略中推荐了这些战术，并将其作为“神经战”的一部分。这些恐怖活动包括‘用电话或信件宣布政府和警察的错误”；让警察获得虚假的计划，以便分散他们的注意力”，“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。暗杀已经被证明是非常有效的一种恐怖活动的工具，也是对目标和社会最有效的一种威吓手段。

(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，把恐怖分子采用最新技术手段在最新领域与人类为敌的恐怖活动称作新恐怖活动。如意大利“长枪党武装”完全是利用高技术的恐怖组织，它目标明确，手段高超，专以突入银行和新闻机构的计算机网络、窃取存储资料、删改程序、散布虚假信息为能事，是典型的针对网络和媒体的恐怖活动。诸如网络恐怖、信息恐怖、电磁恐怖、生态恐怖、金融恐怖、贸易恐怖、文化恐怖、经济恐怖、激光恐怖、基因恐怖等活动都属于新恐怖活动的范畴。

1. 信息恐怖活动。信息恐怖活动，是对计算机网络中的信息系统，通过信息的获取、传递、处理和运用等实施过程的运作，运用信息技术（传感技术、通信技术、计算机技术）围

绕着信息系统的破坏与摧毁实施的恐怖活动。

把网络作为袭击目标的信息恐怖活动，是利用计算机网络技术和手段，围绕网络系统的生存与毁灭进行的恐怖活动。如恐怖分子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而采取的各种恐怖措施和活动。网络恐怖分子施恐多以网络攻击达其削弱、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，实施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。运用病毒的运行机理和破坏机理、病毒渗入系统和网络的方法、无线电发送病毒的方法，运用网络分析器软件驱动嗅探器和硬件磁感应嗅探器等网络嗅探器，运用篡改、窃取和欺骗等信息技术置袭击目标于死地。

信息恐怖活动往往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。尤其是对军队信息系统，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，从而导致敌方作战失败的结局。

电磁恐怖活动，也是信息恐怖活动，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，是指由功率超过 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的干扰技术。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在瞬间遭到严重破坏而完全失灵。

1999 年 1 月 20 日，俄罗斯《消息报》刊登弗·洛巴列夫和尤·帕尔菲奥诺夫两位教授与俄科学院院士弗·福尔托夫合写的一篇文章，提出电磁恐怖主义是 21 世纪的威胁。他们认为，恐怖分子搞恐怖活动的手腕已变得越来越巧妙，所使用的工具中经常可以看到各种各样的电子技术设备。例如，在夺取达吉斯坦基兹利亚尔市的那场战斗中，车臣恐怖分子使用了一种能发射电磁波的仪器，致使警察无法通过无线电同外界联系。1995年 3月在莫斯科，一名罪犯利用一部简陋的，用手工制作的仪器使两家商店的警报装置失灵。

1998年 1月 21 日，《瑞典日报》报道，俄罗斯已研制出便携式强电磁脉冲发生器，能摧毁计算机系统。这种装置如果落入恐怖分子的手中，后果将不堪设想。美国和俄罗斯已有了这种发生器的模型。美国飞利浦实验室所拥有的一部辐射系统，峰值功率为 8000 万瓦，而且向周围空间辐射的并不是像核爆炸那样的单次电磁脉冲，而是连续的脉冲集（每秒频率逾千次）。

恐怖分子则可能利用它来进行以下的活动。

(1)在距机场 5～10公里处的乡间主道停着 一辆厢式货车，车上装有能造成强大的电磁干扰的辐射装置， 致使跑道区域内飞机的无线电系统的工作受到干扰。

(2) 公路旁边的大楼里有一合 电磁脉冲 辐射装置正在工作，由于现代汽车装有具有一定功能的电脑和蕊量 ,在强电磁

辐射的干扰下后果将是灾难性的。瑞典和美国已成功地进行了通过无线电辐射汽车上的电脑使汽车停下的试验。

(3) 如果银行、超市或控制站周围装有辐射源，电磁脉冲的干扰将使这些设施内的电脑系统陷入瘫痪，结果导致工作的混乱。虽说超强电磁脉冲发生器是一种复杂的技术装置，但一般的专家就能制造出来。

只要把高压脉冲接到无线电波束传感器的天线、红外辐射仪、导线及电缆上，保安技术设备就会失灵。可行的方法之一是，在空中所形成的导电微粒范围内传输 10 万伏特左右的电压。

在通信线路和电源的周围以及信息汇集和整理地区制造电磁干扰，就可以引发保安设备错误的接通。持续时间为十亿分之一秒的低功率电磁脉冲发生器最擅长制造这类干扰。另一种方法是使用一种专门的感应器，把这种感应器安装在通信线路和电源线路上即可造成干扰。在无线电用品商店里就能买到这类极其简易的装置。

只要借助到处可以买到的一些无线电元件就可以使报警装置不报警，例如，无线电波相干探测仪在加工所接收的信号时，必须使用辐射信号的复制品，借助一部相似信号干扰装置就能使探测仪变得无用武之地。另外，恐怖分子还可以利用一些操作比较简单的电器元件大搞恐怖活动。动力电缆、变电站、配电盘等东西都很常见，都没有装备现代化的、免受强电脉冲干扰的保护装置。

电磁恐怖活动利用的是非致命的和隐秘的武器，能覆盖大量的目标并且不留痕迹。

2. 生态恐怖活动。生态恐怖活动，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另造局域生态制造灾害等恐怖活动。如制造台风、海啸、地震等。也许不要多长时间，人造“厄尔尼诺”或“拉尼娜”现象就可能成为某些国家或非国家组织手中的又一种制造超级恐怖的超级武器。特别是那些带有恐怖性质的非国家组织，他们不承担对社会和民众的责任，更易成为发起生态恐怖战的主体。而现实的危险在于，为求得尽快的发展速度，全球生态环境经常处于突变的临界线上，任何微小变量的加减，都足以引起一场生态活动浩劫。

3.金融恐怖活动。金融恐怖活动，即利用金融（偷袭）手段进行的恐怖活动。如一场由国际游资拥有者们处心积虑发起的金融偷袭——东南亚金融风暴竟把一个接一个不久前还被世人誉为“小龙”、“小虎”的国家掀翻在地。经济战线的失守，更使社会政治秩序动荡不安，此起彼伏的骚乱造成的伤亡简直不亚于一场局部战争，而对社会机体的伤害程度甚至比局部战争还严重。其中扮演了重要角色的人物是金融恐怖分子乔治·索罗斯。以马来西亚总理马哈蒂尔为代表的一些东南亚国家政界人士和经济学家认为，东南亚金融市场的动荡是完全由乔治·索罗斯等国际金融投机家的炒作造成的。称索罗斯这位美国的基金管理人是因为东盟接纳缅甸为其新成员而要惩罚东南亚国家经济“使国际犯罪活动达到了最高峰”。李登辉趁东南亚金融危机自贬台币，借以打击港币、港股特别是红筹股。这还不算在此番金融饕餮大聚餐中一拥而上的那些大大小小的“炒家”，包括以发表信用评估报告为名，给金融大鳄们揭示打击目标的摩根·斯坦利公司和穆迪公司这类间接参与并获益者。

在1998年的阿尔巴尼亚骚乱中，可以清楚地看到那些富可敌国的巨富和跨国集团设立的各种基金会的作用，这些基金会控制媒体、资助政治组织与当局对抗，致使国家秩序崩溃、合法政府倒台，可称之为基金会式的金融恐怖战。

4. 贸易恐怖活动。贸易恐怖活动，即利用贸易手段进行的恐怖活动。如果说“贸易战”在十几年前还只是一个形容词，今天的它却实实在在成了许多国家手中的非军事性战争的工具，也成了恐怖分子施恐的手段。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 301 条款，最惠国待遇等。其中任何一种手段产生的破坏性效果都不亚于一次军事活动。

5. 文化恐怖活动。文化恐怖活动，即恐怖主义与文明冲突相结合所进行的恐怖活动，是国际恐怖活动的一种形式。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、恐怖组织或者国家都可能制造文化恐怖活动。它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一个“工具”，许多情况下，其后果之一是冲突中的文化因素转化为宗教因素。

文化恐怖活动的著名案例有：2001 年“9·11”恐怖袭击案；2001 年阿富汗巴米杨大佛被毁事件； 1992 年印度阿约迪亚清真寺被拆毁事件；1989 年拉什迪事件；1979 年穆斯林狂热分子占领麦加大清真寺事件；1969 年火烧阿克萨清真寺等。

文化恐怖活动具有跨国性、长期性、行为主体的多样性三大特点，增加了预防的困难性和复杂性。

6. 经济恐怖活动。经济恐怖活动，即利用那些有组织爆炸、劫持人质、恐吓或暗杀等暴力性的，或所谓的“有组织”犯罪形式，渗透到经济及合法经济活动领域的恐怖活动。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、恐怖、丧失信心、麻痹和社会意志消沉，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.激光恐怖活动。激光恐怖活动，即利用激光技术手段进行的恐怖活动。比如，想袭击一架飞机，想剥夺一辆坦克的作战能力，可以用炮弹、导弹去摧毁它，也可以用激光束去毁坏其光学设备或是使乘员致盲。在战场上，一个伤员比一名阵亡者需要更多的照料。杀伤人员可以剥夺敌人的战斗力，让敌人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更多一些想像力。

8.基因恐怖活动。基因恐怖活动，即利用基因技术手段（武器）进行的恐怖活动。基因技术是高新技术。基因技术为人类提供很多需求，尤其在医学中，对人类的贡献很大，但基因技术的负面效应可能被恐怖组织（分子）用作施恐手段的技术依托，制造未来生物战的恐怖杀手——基因武器。

基因武器有别于传统武器的特点：

(1) 威力巨大的杀伤性。如前苏军研制出的一种基因毒素，只需 1 克就能毒杀 10 亿只猫。将常见的肉毒毒素基因转移拼接到另一种特殊基因上，制造了一种名为“热毒素”的毒素基因武器，只需 20 克就足以使全球 50 亿人死于一旦。美军研制的一种超级出血热基因武器，若投入敌方水系，可使整个流域的军民丧生或失能。

基因武器威力巨大，但成本极低。有人计算，用 5000 万美元建立 1 个基因武器库，其杀伤能力将远远超过价值 50 亿美元的核武器库。基因武器对人类危害是巨大的。“黑死病”

曾遍及欧洲，流感、霍乱曾世界大流行，艾滋病已扩散到世界五大洲。

（2）使用方便，保密性极强。在未来生物战中，可能采用人工、飞机、火炮、火箭、炸弹、导弹、气球、舰艇及潜艇等各种方法对敌方实施基因武器攻击，使敌方人体组织和生活环境遭到破坏，导致一个民族、一个国家丧失战斗力，在不流血中被征服；也可能使被攻击的民族失去正常智力，甚至代代相传却浑然不觉，从而长期变为侵略者的殖民地；也许经过几年的种族清洗后，受害者才会觉察到有人在他们身上使用了基因武器，但为时已晚；基因武器可以改变一个国家或一个种族的基因，进而会影响一个洲，甚至全球人群的基因稳定。基因武器就像一把特制的加密锁，只有研制设计者方知道其遗传密码，才能打开这把奇锁，而对方很难窥破其秘密加以控制和防范，这就使基因武器比经典生物武器具有更好的保密性能。

（3）制造生物威慑，引发恐怖心理。现代战争越来越注重心理战，以强烈的威慑给对方制造恐怖。基因武器是制造心理恐怖引发社会动荡的最理想选择。

首先，这种恐怖心理来自对历史惨剧的回忆。正如人们提及核武器便联想到广岛、长崎可怕的磨菇云，提及化学武器便联想到奥斯维辛集中营纳粹分子毒杀几百万犹太人一样，提及生物武器自然会联想到日军 731 细菌部队的杀人魔窟，心理恐怖油然而生。

第二，恐怖心理来自于致死性传染病的威胁。一旦烈性传染病暴发流行，国家就会迅速采取封锁和隔离措施，并投入大量人力、物力从事医疗防疫工作。进而使得生产停顿、交通中断、兵员不能调动，严重影响生产和作战能力，并影响公民情绪和军队士气。

第三，恐怖心理来自于一般公众对基因武器的陌生感、神

秘感和恐怖感。使用（或威胁使用）基因武器将会触发人的强烈生理反应及自我暗示，使人出现肌肉紧张、心动过速、呼吸加快、出汗、颤抖等一系列病状和体征，大量涌入医疗机构救助，由于对看不见、摸不着的生物武器的恐惧，导致心情紧张（害怕传染）、情绪沮丧，甚至精神崩溃 进而会使全社会人心惶惶，谣言四起，惊惶失措，最终有可能引发社会动荡。

总之，基因武器可以在战时或和平时期，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。

（三）超级恐怖活动

尽管当前恐怖活动还大多使用常规手段，但是 1995 年 3 月日本奥姆真理教在东京地铁内实施的“沙林”毒气谋杀案及 1998 年 4 月在东京郊区发生的煤气谋杀案，已给人们敲响警钟。恐怖分子可获得的大规模杀伤性武器包括：核装置、细菌武器、毒气武器及各种超级杀伤病毒。由于生化武器从原材料到价格以及制造使用方面并不像核武器那样难。因此人们十分担心，一旦恐怖分子使用生化武器进行恐怖活动，将造成难以估量的后果。所以，人们把使用包括生化武器在内的大规模杀伤武器的恐怖活动称为“超级恐怖活动”。

1998 年，德国《欧洲安全》月刊第 8 期刊登维尔弗里德·赫而曼的一篇文章，题为《“超级恐怖主义”——21 世纪的挑战》，提出了这样的看法：恐怖分子在世界范围内越来越多地使用生化武器。1995 年，日本东京地铁的沙林毒气事件并非个别情况。有关统计表明，自 1950 年以来，已经发生过 270 多起使用生化剂的事件。例如， 1997 年澳大利亚的一些百货商店遭到氯化氢袭击。德国、巴西和美国的一些食品被下毒，恐怖分子使用的物品繁多，从砷、芥子气、氯化物（化学物