第5章 人员安全与情报

信息安全管理

主讲 李章兵

教学目标

- 本章的重点
  - 人员安全管理原则
  - 人员安全管理措施
  - 内部人员安全管理
  - 授权管理

教学内容

- 5.1 人员安全管理概述
- 5.2 人员安全管理原则
- 5.3 人员安全管理措施
- 5.4 内部人员安全管理
- 5.5 授权管理
- 5.6 情报与分析

5.1 人员安全管理概述

- 人员管理
  - 指依据公共组织编制法规，按照公共管理职能调整和机构设置的需要，通过法定程序，确定管理人员数额、结构比例、领导职数。
  - 是公共组织编制管理的核心内容。
  - 精要是将合适的人员配备到合适的职位上，并让其从事合适的工作，从而实现“人适其位，位得其人”。

5.1 人员安全管理概述

- 人员安全管理
  - 指与组织或企业的业务信息系统相关的人员的安全管理。
    - 信息系统安全问题中最核心的是管理问题。
    - “人”是实现信息系统安全的关键因素。
  - 对企业信息系统的人为威胁主要来自：

5.1 人员安全管理概述

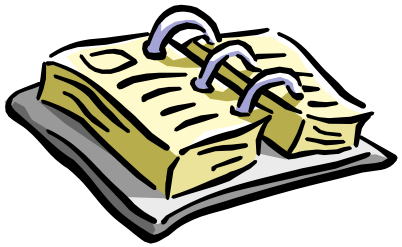
- 内部人员：
  - 组织机构的组成人员。更能直接攻击重要目标，逃避安全检查。
    - 一般都具有对系统一定的合法访问权限
    - 对系统内重要信息存放地、信息处理流程、内部规章制度等比较了解，比外部人员拥有更大的便利条件。
- 准内部人员：
  - 硬件厂商、软件厂商、软件开发商
  - 程序开发人员、维护人员
    - 对系统情况有一定的了解，一定时期内对系统具有的合法访问权限；
    - 是专业人员，更有条件和能力对系统设置后门和入侵。

5.1 人员安全管理概述

- 特殊身份人员：
  - 一般包括记者、警察、技术顾问和政府工作人员
    - 可能会利用自己的特殊身份了解系统，以作相应改动。
- 外部个人或小组
  - 外部访问者
    - 由于Intranet的操作系统、数据库管理系统及通信设备等安全级别不够，容易遭到外部黑客的攻击。
- 竞争对手
  - 各商家或竞争对手
    - 可能派出商业间谍，或采取高科技手段，向竞争企业的网络发起进攻。

5.1 人员安全管理概述

- 人员安全管理的基本内容
  - 人员安全管理原则
  - 人员安全管理措施
  - 人员安全管理是信息安全管理的重要部分
    - 公安部曾做过统计，70%的泄密犯罪来自于内部；电脑应用单位80%未设立相应的安全管理体系；58%无严格的管理制度。



5.2 人员安全管理原则

- 人员安全管理原则
  - 多人负责原则
    - 即每一项与安全有关的活动，都必须有2人或多人在场。
  - 任期有限原则
    - 任何人最好不要长期担任与安全有关的职务，以保持该职务具有竞争性和流动性。
  - 职责分离原则
    - 出于对安全的考虑，科技开发、生产运行和业务操作都应当职责分离。

5.2 人员安全管理原则

- **职责分离原则**
  - **职责分离是威慑和预防欺诈或恶意行为的一种手段。**
  - **避免不能及时地发现日常业务的错误情况。**
  - **避免一个人负责多个关键的职位**
  - **使相关人员的访问对象和权限受限。**
    - **对计算机、生产数据资料库、生产程序、编程文档、操作系统及其工具的访问受到一定的限制，某一个人的潜在破坏行为就被减弱。**

职责分离矩阵

	控制组	系统分析员	应用程序员	帮助台和支持经理	最终用户	数据录入员	计算机操作员	数据库管理员	网络管理员	系统管理员	安全管理员	系统程序员	质量保证人员
控制组		X	X	X		X	X	X	X	X		X	
系统分析员	X			X	X		X				X		
应用程序员	X			X	X	X	X	X	X	X	X	X	
帮助台和支持经理	X	X	X		X	X		X	X	X		X	
最终用户		X	X	X			X	X	X			X	X
数据录入员	X		X	X			X	X	X	X	X	X	
计算机操作员	X	X	X		X	X		X	X	X	X	X	
数据库管理员	X		X	X	X	X	X		X	X		X	
网络管理员	X		X	X	X	X	X	X					
系统管理员	X		X	X		X	X	X				X	
安全管理员		X	X			X	X					X	
系统程序员	X		X	X	X	X	X	X		X	X		X
质量保证人员		X	X		X							X	

X—表示职能合并可能会产生潜在的控制风险

5.2 人员安全管理原则

- 职责分离原则
  - 对职责分离的控制
    - 交易授权（Transaction Authorization）
      - 交易授权是用户部门的责任，对部门中负责有一定责任的相关人员进行一定程度的授权，使其可以正常进行交易。
      - 管理层和审计师必须定期检查交易记录的授权。
    - 资产保管（Custody of Assets）
      - 组织必须确保资产保管责任，并对保管责任进行适当的分派。
      - 通常要对特定的部门指定数据所有者，数据所有者的职责应当以书面方式具体记录。
      - 数据所有者有责任决定对数据的使用者授予什么级别的访问权限，从而提供充分的安全，管理组通常负责实施和强化安全体系。

5.2 人员安全管理原则

- 职责分离原则
  - 对职责分离的控制
    - 数据访问（Access to Data）
      - 对数据访问的控制是通过在用户场所和IPF综合，采用物理层、系统层及应用层的安全措施组成。
      - 物理环境必须被有效保护，防止未经授权的人员接触与中央处理单元连接的各种有形设备。还应该在系统层和应用层采取进一步的安全措施，防止未经授权的人员访问组织的重要数据。
      - 组织应当基于其安全策略和通用的实践标准（如：职责分离、最小授权原则）来决定其访问控制决略。
      - 实施控制措施不能以中断正常业务为代价，也不能给管理人员、审计师及用户增加太多负担。
      - 对重要数据的访问控制必须加以限制，所采取的控制措施必须能保护组织的所有信息资源。这就要求组织首先对信息资产进行分类，定义信息资产的敏感性级别。

5.2 人员安全管理原则

- 职责分离原则
  - 对职责分离的控制
    - 授权表单（ **Authorization Forms**）
      - 交易授权是用户正常交易的保证；
      - 交易授权以表单形式申请、授权和记录。
    - 用户授权表格（ **User Authorization Tables**）
      - 信息系统部门应当使用授权表单中的数据建立和维护用户授权表格。
      - 确定谁有权更新、修改、删除和查看数据。这些访问权限分别在系统级、交易级甚至字段级实现。

5.2 人员安全管理原则

- 职责分离原则
  - 职责分离可能造成的风险
  - 小型组织或企业可职责分离的人员少
    - 部门可能仅由四-五个人组成；
  - 职责分离的补偿控制包括：
    - 审计跟踪。
    - 核对
    - 例外报告
    - 事务处理日志/交易日志
    - 监督性审核
    - 独立性审核

5.2 人员安全管理原则

- 职责分离的补偿控制
  - 审计跟踪
    - 审计跟踪是所有设计优良的系统的基本组成部分。
    - 通过追踪一项事务处理的详细流程(“地图” --来龙去脉），审计师能够建立实际事务自起点到终点的处理全过程。
    - 审计跟踪确认：启动该事务处理的人和时间、处理数据录入的日期和时间、记录的类型和文件更新等。
  - 核对
    - 绝大多数情况下数据核对是用户的责任。
    - 应用程序可以有限核对数据，使用控制总计和平衡表来完成验证，增加了应用程序成功运行、数据正确平衡的置信度。

5.2 人员安全管理原则

- 职责分离的补偿控制
  - 例外报告
    - 由主管层来处理，并且需要证据，如处理签名和日期；
    - 管理层还应当确保例外被及时处理。
  - 数务处理日志/交易日志
    - 手工方式或自动方式记录日志。
    - 手工日志可以是交付处理之前的一份交易记录；自动事务处理日志提供了所有被处理的事务记录，并且保存在计算机系统中。
  - 监督性审核
    - 监督性审核可以通过现场观察和问询进行。
  - 独立性审核
    - 独立性审核帮助发现错误或违规行为。
    - 可以对错误或故意违反操作程序的行为进行补偿控制。
    - 独立性审核在不能进行职责分离的小型组织中尤为重要。

5.3 人员安全管理措施

- 人员安全管理措施包括
  - （1）领导者安全意识
  - （2）系统管理员安全意识
  - （3）一般用户安全意识
  - （4）外部人员安全管理
  - （5）内部人员安全管理
- 重要的是内部人员的安全管理。

5.3 人员安全管理措施

- **1.领导者安全意识**
  - 定期制订安全培训计划，组织安全学习活动；
  - 责成各级高层管理人员经常关注和强化计算机安全技术和保密措施；
  - 组织计算机安全任务小组来评定整个系统的安全性，安全小组应及时向高层管理层报告发现的问题并提出关键性建议；
  - 领导者可授权安全小组制定各种安全监督措施。
  - 管理层对违反安全规则的人员应进行惩罚。
  - 领导者应严于律己，不得将内部机密轻易泄漏给他人，尤其注意收发电子邮件时，不将企业专有信息放在网络服务器和FTP服务器上。

5.3 人员安全管理措施

- **2.系统管理员安全意识**
  - 保证系统管理员个人的登录安全。
  - 给账号和文件系统分配访问权限。
  - 经常检查系统配置的安全性。如线路连接及设备安全、磁盘备份是否安全等。
  - 注意软件版本的升级，安装系统最新的补丁程序，尽量减少入侵者的窃取到口令的文件的可能性，关掉不必要的服务，减少入侵者入侵途径。

5.3 人员安全管理措施

- **3.一般用户安全意识**
  - 经常参加计算机安全技术培训，学习最新安全防护知识。
  - 以合法用户身份进入应用系统，享受授权访问信息。
  - 不与他人共享口令，并经常更换口令。
  - 不将一些私人信息，如公司计划或个人审查资料存入计算机文件。
  - 注意将自己的主机设为拒绝未授权远程计算机的访问要求。
  - 保证企业的原始记录，如发票、凭证、出库和入库单等不被泄露。
  - 自觉遵守公司制定的安全保密规章制度，不制作、复制和传播违法违纪内容，不进行危害系统安全的活动。

5.3 人员安全管理措施

- **4.外部人员管理**
  - 程序员(准内部)：企业应监视和分析系统维护前后源代码及信息系统运行情况，防止开发维护人员的破坏行为。
  - 特权层：将特殊身份人员（如警察、记者等）的权限限制在最小范围。
  - 对手与间谍：密切注视竞争对手的近况，防止商业间谍偷袭。

5.4 内部人员安全管理

- 内部人员制定安全管理制度
  - 三种情况分别制定

5.4 内部人员安全管理

- 1.员工雇佣前
  - (1).人员安全审查
  - 安全审查是人员控制的非常重要措施。
    - 在招聘新员工或员工升迁时安全审查；
      - 人才市场上假文凭、假履历满天飞。
      - 各种权学交易、钱学交易的博士硕士班泛滥成灾。
  - **审查对象：**
    - **信息系统的分析和管理人员，单位内的固定岗位人员，临时人员或参观学习人员等。**
  - **审查范围：**
    - **人员安全意识、法律意识和安全技能等。**

5.4 内部人员安全管理

- 1.员工雇佣前
  - (1).人员安全审查（政治与业务能力）
  - 人员背景调查措施
    - 政治思想方面的表现。
    - 对申请人的学历、履历的审查（完整性和准确性）。
    - 对其所宣称的学术和职业资质进行确认。
    - 单独的身份认证（护照相应身份证明文件）。
    - 性格测试。
    - 信用记录调查。
    - 身体状况调查等。

5.4 内部人员安全管理

- 1.员工雇佣前
  - (2).人员岗位审查标准
    - 必须根据信息系统所规定的安全等级确定审查标准。
    - 信息系统的关键岗位人选，必须经过严格的政审并要考核其业务能力。
      - 如安全负责人、安全管理员、系统管理员和保密员等
    - 因岗挑选人，制定选人方案。遵循“先测评、后上岗；先试用、后聘用”原则。
    - 所有人员都应遵循“最小特权”原则，并承担保密义务和相关责任。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (1)入职培训
  - 入职前必须实施职位培训
  - 培训方式：
    - 内部培训、外部培训、实习、自学考试、学术交流。
    - 采用不同媒体来宣传信息安全，如公司邮件、网页、视频。
  - 培训内容：
    - 安全规则的可视化执行。
    - 模拟安全事故以改善安全规则。
    - 员工通过签订保密协议，了解安全需求。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (1)员工安全管理
  - 员工安全工作职责
    - 将组织安全政策中所设定的安全角色和安全责任记录到员工工作职责说明书中。
    - 从新员工签订合同时起，强化员工的信息安全意识。
    - 通过适宜的方式把相关的安全责任要求传达到每一个员工，使其理解并遵照执行。
    - 确保所有员工、合同方和第三方用户了解信息安全威胁和相关事宜、他们的责任和义务，并在他们的日常工作中支持组织的信息安全方针，减少人为错误的风险。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (1)员工安全管理
  - 组织管理职责
    - 在被授权访问敏感信息或信息系统前知道其信息安全角色和方法。
    - 从组织获得声明他们角色的安全期望的指南。
    - 被激励以实现组织的安全方针。
    - 对于他们在组织内的角色和职责的相关安全问题的意识程度达到一定级别。
    - 遵守雇佣的条款和条件，包括组织的信息安全方针和工作的合适方法。
    - 持续拥有适当的技能和资源。

5.4 内部人员安全管理

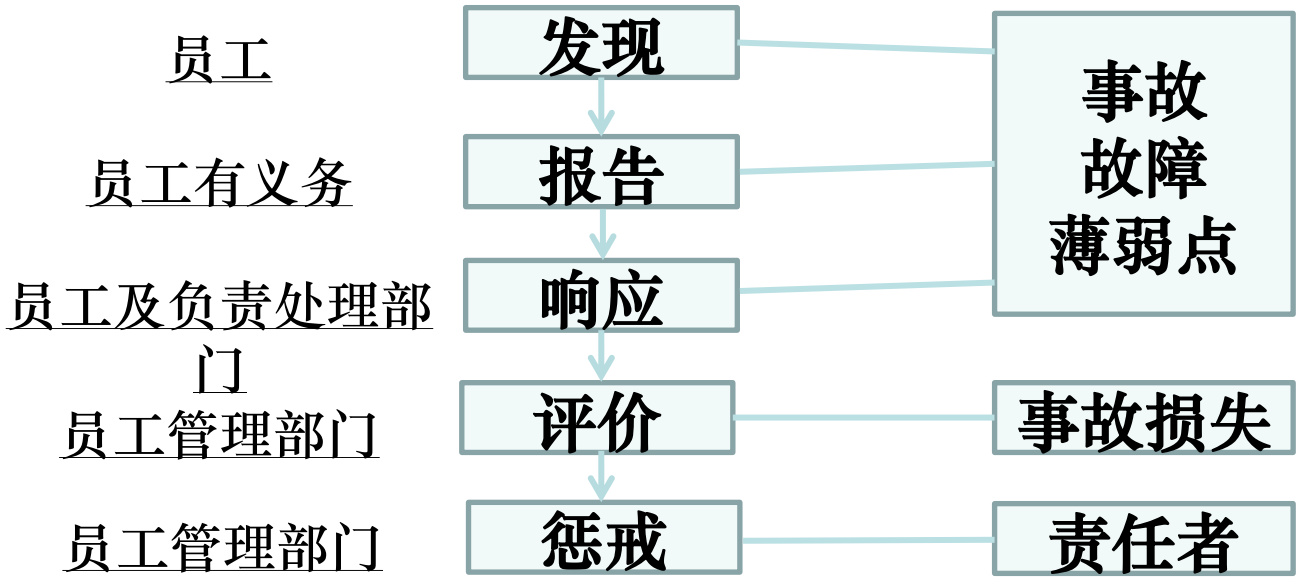
- 2.员工雇佣中
  - (1)员工安全管理
  - 员工主要考核
    - 思想政治方面考核
      - 是否遵守法律、法规，执行政策、纪律和规章制度，履行职业道德、劳动服务态度等。
    - 业务、工作成绩考核
      - 依据各自的职责进行考核，相关人员不仅要有业务理论水平还要有实际操作技能。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (1)员工安全管理
  - 员工惩戒：违反安全的惩戒原则
    - 惩戒之前：验证安全违规的过程。
    - 惩戒过程：应确保正确公平对待疑违规的雇员。
      - 正式惩戒过程应规定一个分级响应，要考虑诸如违规的性质、重要性及对业务的影响等因素。
      - 对于严重的明知故犯情况，应立即免职、删除访问权限和特权，如果需要可直接带离现场。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (2)安全事故与安全故障反应机制
    - 安全事故和故障反应过程



5.4 内部人员安全管理

- 2.员工雇佣中
  - (2)安全事故与安全故障反应机制
  - 反应机制--确保及时发现问题
    - 建立有效的管理渠道或程序
      - 确保员工及时发现并报告安全事故、安全故障或安全薄弱点，以便迅速对其作出响应。
    - 正式报告的程序内容包括：
      - 明确报告的受理部门
      - 报告的方式，如专用电话、书面报告
      - 报告内容要求，如事故发生的时间、地点、系统名称、威胁、后果等。
      - 处理事故的反馈要求，以便从中吸取教训。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (2)安全事故与安全故障反应机制
  - 反应机制--对于安全事故的响应
    - 针对不同类型的安全事故，作出相应的应急计划，规定事故处理步骤。
    - 对事故、故障、薄弱点作出迅速、有序、有效的响应，减少损失。
      - 信息系统受到的软件和硬件故障威胁
        - » 用户应记录有关故障的信息，及时报告主管部门；
        - » 由有关技术人员进行故障排除，并分析故障原因，采取必要措施，防止类似故障发生。
      - 员工记录发现的安全薄弱点，按照规定的报告方式向有关部门报告
        - » 无论是管理上的、技术上的，还是信息系统本身存在的，由相关部门对可疑的薄弱点进行确认，从而确定相关资产的风险程度，选择相应的控制措施并实施。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (2)安全事故与安全故障反应机制
  - 反应机制--从事故中吸取教训
    - 安全主管部门应调查确认安全事故或故障，形成事故或故障评价资料。
      - 对事故或故障的类型、严重程度、发生的原因、性质、产生的损失、责任人进行确认和评价
    - 总结信息安全事故或故障的经验、教训，作为安全教育和培训的案例
      - 组织内部人员从已发生的事故案例中学习。

5.4 内部人员安全管理

- 2.员工雇佣中
  - (2)安全事故与安全故障反应机制
  - 反应机制--建立惩戒机制
    - 建立一种安全惩戒管理办法
      - 明确规定员工被惩戒的适用情况、证据提供、惩戒手段、审批等具体要求，确保准确、公正、合理处理违反方针、程序和有关安全规章的员工。
    - 惩戒手段包括：
      - 行政警告、经济处罚、调离岗位、依据合同予以辞退
      - 对于触犯刑律者应交由司法机关处理

5.4 内部人员安全管理

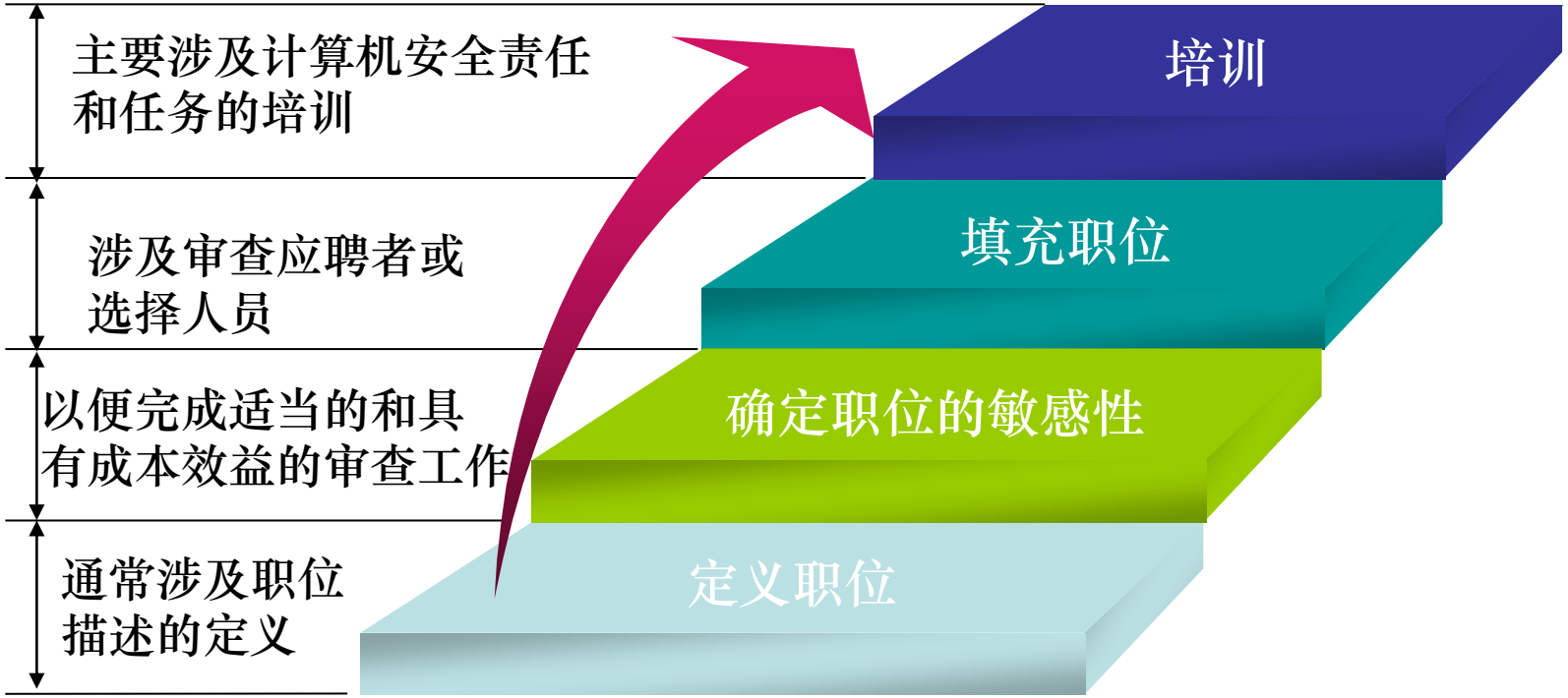
- 3.员工雇佣的终止和变更
  - 雇佣、合同或协议终止时的安全措施
    - 员工、合同方和第三方应归还所使用的组织资产。
      - 如公司文件、设备、信用卡、访问卡、软件、手册和存储于电子介质中的信息等。
    - 应确保所有有关的信息已转移给组织，并且已从雇员、合同方或第三方设备中安全删除。
    - 当一个雇员、合同方或第三方用户拥有的知识对正在进行的操作具有重要意义时，此信息应形成文件并传达给组织。
    - 应撤销所有员工、合同方或第三方用户对信息和信息处理设施的访问权限，或根据变化调整。
      - 比如删除密钥、ID卡、签名等文件，更改账户密码等。

5.5 授权管理

- 组织授权
  - 大量安全问题关系到人员如何与计算机进行交流以及他们工作所需的权限。
  - 原则：业务所需，分级授权，最小权限
- 主要考察几类人员：
  - 岗位人员：与计算机系统进行交流，管理业务
  - 系统用户：影响组织业务。
  - 承包人或公众：访问系统时需要考虑的特殊因素。

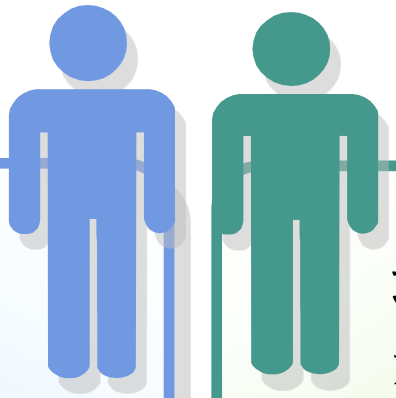
5.5 授权管理

- 1.职员授权管理
  - 安排职员通常涉及的四个步骤：



5.5 授权管理

- 1.职员授权管理
  - (1).定义职位
    - 负责业务的岗位。
      - 定义职位的早期应识别和处理安全问题。
    - 职位一旦被定义后，负责的主管应确定职位所需的访问类型。



职务分离原则：是指对角色和责任进行分类使单独一个人无法破坏关键的过程。

最小特权原则：是指只赋予用户其执行工作任务所需的访问权。

5.5 授权管理

- 1.职员授权管理
  - (2).确定职位敏感性
    - 了解这一职位所需的知识和访问级别。
    - 敏感性确定
      - 传统因素：如对保密信息的访问和受托责任。
      - 该人员通过滥用计算机系统可能造成损害的类型和程度
        - » 如泄漏私人信息、中断关键处理、计算机欺诈
    - 控制职位敏感性程度
      - 职位敏感性过度设定会浪费资源，而过小设定可能会造成无法接受的风险。

5.5 授权管理

- 1.职员授权管理
  - (3).填充职位
    - 确定敏感性职位后，准备填充职位(配置人员)。
    - 公布正式的空缺职位公告；
    - 识别符合职位需求的申请者。
    - 比较敏感的职位通常需要雇佣前的背景审查。
    - 审查涉及的因素：
      - 犯罪记录
      - 工作和教育经历
      - 个人方面
      - 拥有和使用的非法物品记录

5.5 授权管理

- 1.职员授权管理
  - (4).员工培训
    - 被雇佣后成为组织员工。
    - 员工培训包括计算机安全责任和任务的培训。
    - 良好培训的员工对于计算机系统和应用发挥效率起到至关重要的作用。

5.5 授权管理

- 2.用户管理
  - 用户对于计算机访问权的体现在账户，有效管理账户对于维护系统安全是很重要的。
  - 用户账户管理主要是识别、认证和访问授权。
  - 用户账户管理内容

5.5 授权管理

- 2.用户管理
  - 用户账户申请
    - 用户主管向系统管理员申请系统账户。
    - 系统管理员根据账户申请为新用户创建账户，并被设定所选择的访问授权。
    - 账户信息发给职员，包括账户的识别符（如用户ID）和认证方法（如口令或智能卡）。
    - 当要关闭员工账户时，用户主管通知应用管理员和系统管理员及时撤销或清除账户。

5.5 授权管理

- 2.用户管理
  - 跟踪用户及其访问权限
    - 设定责任所必须的访问权限以维护最小特权原则
    - 了解用户相应的权限，并跟踪其访问权限变更。
  - 集中管理用户的访问过程
    - 审计和管理检查
      - 检查每位人员所拥有的访问权
      - 检查对最小特权原则的符合性
      - 所有账户是否处于活动状态。
      - 管理授权是否处于更新状态。
      - 是否完成所需的培训。

5.5 授权管理

- 2.用户管理
  - 探测非授权活动
    - 审计和审计跟踪用户的权限变动。
    - 要求实施者经常到场(防止缺席期间发生欺诈行为)。
    - 强制关键系统和应用人员休假(调查其是否有给授权和非法活动)。
- 3.临时任命和部门内调动
  - 对用户的访问权限进行相应更改。
    - 如暂时的或永久的更换工作角色、离职等。
  - 信息系统应保持用户访问授权的更新状态。

5.5 授权管理

- 4.离职
  - 分为“友好的”和“不友好的”
  - 友好离职
    - 发生在员工自愿调任、辞职以便接受更好的职位或是退休情况下。
    - 应为离职员工完成一系列标准规程，以确保系统帐户能够被及时清除。
      - 由每个相关功能管理人签署的表格。一般包括管理访问控制、钥匙控制、报告机密和隐私责任、财务管理等。
      - 确认数据的继续可用性。
      - 保证数据的机密性。
    - 用户友好的终止

5.5 授权管理

- 4.离职
  - 不友好的离职
    - 不情愿或敌对情况下的员工离职，包括用户被解雇、裁员或非自愿调任。
    - 不友好离职的风险和威胁
      - 离职的紧张关系导致安全问题的加重和复杂化，可能对信息系统造成损害。
      - 有能力更改代码或改变系统或应用的人员；
      - 一般用户。
    - 账户终止措施
      - 解雇：在通知员工离职时（或之前）清除系统访问权。
      - 辞职：如果有理由预期是不友好离职，应立即终止其系统访问权。
      - 在“布告”阶段，有必要限制人员的活动区域和功能。

5.5 授权管理

- 5.承包人访问
  - 组织或企业使用承包人和顾问协助其进行计算机处理。
  - 使用期限经常比员工短，可能会改变执行审查的成本效益。
  - 承包人员的频繁转换增加了安全项目用户管理方面的开销。
  - 跟踪承包人的访问过程。

5.5 授权管理

- 6.公众访问
  - 设计、开发和使用面向公众散发信息的公众访问系统。
  - 公众访问一般不需要账户，只查询公共信息。
  - **额外的安全问题：**
    - **公开了电话号码和网络访问ID**
    - **通常是匿名的，使系统安全管理复杂化**
    - **增加了对公众访问系统的威胁**
    - **安全管理难度增加**

5.5 授权管理

- 7.相关安全费用审计
  - 审查费用：
    - 初始背景审查和适时定期更新的费用。
  - 培训和意识培养费用：
    - 培训费用包括评估、培训材料、课程费用等。
  - 用户管理费用
    - 管理识别和认证的费用。
  - 授权管理费用
    - 帐户初始建立以后，维护用户现时和完整访问的持续费用。
  - 审计费用
    - 使用自动化工具或人工检查来发现和解决安全问题

5.6 情报与分析

- 1. 情报
  - 情报是通过秘密手段搜集来的、关于敌方外交军事政治经济科技等信息。
  - 情报是被传递、整理、分析后的信息。
  - 情报是为实现主体某种特定目的，有意识地对有关的事实、数据、信息、知识等要素进行劳动加工的产物。
- 情报的作用
  - 误导敌方行动错误或资源部署失当；
  - 指导己方正确行动和资源部署。

5.6.1 情报概述

- 情报属性
  - 目的性、意识性、附属性和劳动加工性是情报最基本的属性
    - 它们相互联系、缺一不可，情报的其它特性则都是这些基本属性的衍生物。
  - 简明扼要是情报的第一要素。
  - 情报具有三个基本属性：
    - 知识性、传递性、效用性
    - 还具有社会性、积累性、与载体的不可分割性以及老化等特性。

5.6.1 情报概述

- 情报分类：军事、商业
- 情报机构
  - 命名
    - 官方：XXX情报局、情报部、安全局、调查局、后勤服务部、调查统计局、保密局
    - 民间：XXX信息所、信息咨询公司、信息事务所
- 情报来源
  - 间谍秘密收集并分析推理
  - 公开信息收集并分析

5.6.1 情报概述

- 间谍
  - 间谍是被派遣或收买来从事机密刺探、情报侦查活动的特工人员。
  - 间谍分类
    - 军事间谍和工业间谍(或称商业间谍)
  - 间谍公开身份
    - 商人、学者、官员、外交官、记者、专家
  - 间谍主要任务
    - 采取非法或合法手段、通过秘密或公开途径窃取情报。

5.6.1 情报概述

- 间谍
  - 间谍活动
    - 通过普通的工作、生活从事间谍活动
    - 间谍可能就在身边
    - 间谍危害后果有轻重，但间谍危害大小与身份无关
  - 间谍来源
    - 本国培训；招募对象国的公民或组织的内部人员。
    - 发展和策反间谍：
      - 目标人物：留学生、专家、官员及其家属、技术人员、商人等
    - 发展和策反手段：
      - 胁迫控制：贴靠刺探、跟踪监视、钓鱼执法、绑架；
      - 利诱哄骗：高薪聘请、美女色诱、技术成果诱骗、荣誉地位诱惑等
      - 设置陷阱：利用人性的弱点。假扮成志愿者、交朋友、帮助联系老师、帮助找工作、帮助租房子等非常友善的方式潜移默化的影响与渗透。

5.6.1 情报概述

- 情报传递
  - 情报传递应尽可能保证间谍的身份不暴露。
  - 情报明文传递：秘密通道明文传递
  - 情报密文传递：公共媒介隐写传递
    - 媒体：文字、图片、声音、视频、博客
      - 特定广告、寻人启事、热点新闻评论、转发评论
    - 介质：纸张、景色、名画、歌曲、音乐、手机
      - Web、网络通信软件
    - 隐写方法：通过变换将情报隐藏于媒体中
  - 发布传递：公开或指定位置和介质
    - 孙子兵法：因间、内间、反间、死间、生间
  - 获取解密：获取后通过约定密钥解密。

5.6.2 情报收集

- 窃密与反窃密
  - 窃听与反窃听
    - 窃听技术
    - 反窃听技术
  - 窃照与窥视技术
    - 窃照
    - 窥视

5.6.2 情报收集

- 1.窃听技术概论
  - 间谍物品-内藏窃听器

克格勃

美国中情局

5.6.2 情报收集

- 1.窃听技术概论
  - 情报侦察工作的地位
    - 当今的信息世界，信息的占有直接反应了一个国家的综合国力。
    - 为在新的国际竞争中取得有利地位，各国都发展和强化情报工作。
      - 美国国家安全局（NSA）的电子窃听网络包括全球
      - 导弹的精确位置、首相或总统的私下谈话、毒枭的密谈
    - 使用窃听高技术手段，综合各种技术并交替使用。
      - 更新升级窃听技术。

5.6.2 情报收集

- 1.窃听技术概论
  - 窃听技术是在窃听活动中使用的窃听设备和窃听方法的总称。
  - 使用者：国家官方机构、社会团体、个人。
  - 主要窃听技术
    - 电话窃听
    - 无线窃听
    - 微波窃听
    - 激光窃听

5.6.2 情报收集

- **1.窃听技术概论**
  - 窃听技术发展史

5.6.2 情报收集

- 2.窃听技术
  - 电话窃听

    - 落入式电话窃听器
      - 可以当作标准送话器使用
      - 拿起话筒时它就将通话内容用无线电波传输给几百米外窃听的接收机。
    - 搭线窃听原理（非模拟信号）
      - 在架空电话明线上安装两只伪装成绝缘瓷瓶的窃听器，跨接在电话线上。
      - 一只装有窃听感应器、发射机和蓄电池；另一只装有窃听感应器和蓄电池。当线路上通过电话、电报、传真信号电流时，经过两个窃听感应器，将感应信号送到发射机
      - 固定在架线杆顶部的天线将信号发射出去，被约1公里以外的接收机接收。蓄电池是太阳能电源，能长期使用。

5.6.2 情报收集

- 2.窃听技术
  - 电话窃听
    - 电话用窃听发射机：米粒大小，装在电话机内或电话线上，电话拨通时才工作。
      - 70年代美国“水门窃听事件”使用。

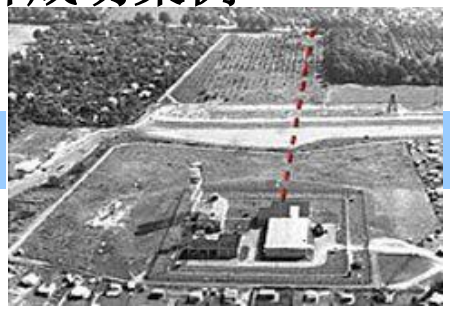
民主党全国总部当时所在地水门大厦

尼克松因此事垮台

5.6.2 情报收集

- 2.窃听技术
  - 电话窃听—室内谈话窃听
    - 国外广泛使用，利用谐波窃听器
    - 利用另一部电话，对准目标房间的电话进行遥控。
    - 当目标电话中的“无限远发射器”收到遥控信号时，自动启动窃听器，可以远距离窃听室内人谈话。
    - 无限远指电话线路。
      - 20年代西柏林的“地下隧道”窃听，美国中央情报局的有线电话窃听成功案例

柏林隧道



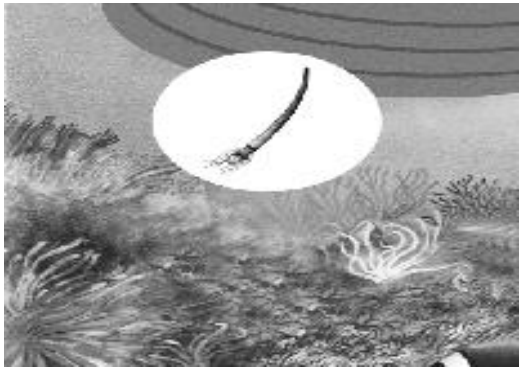
苏军总部

5.6.2 情报收集

- 2.窃听技术
  - 无线窃听
    - 70年代开始，大规模集成电路和微电子技术发展
    - 间谍情报活动广泛应用
    - 原理：
      - 由传声器所窃取的谈话信号，不经过金属导线，而通过无线电波送到窃听装置的接收机上。
      - 无线窃听接收机接收到这些无线电波后，经过检波、滤波、放大，把窃听信号还原出来，或用录音机记录下来。
    - 窃听器体积微型化
      - 隐藏在钢笔、手表、打火机、鞋跟、人体器官内。
    - 自我保护功能：
      - 当知道有人检查窃听设备时，可以遥控停止窃听器工作。

5.6.2 情报收集

- 2.窃听技术
  - 无线窃听
    - 窃听器“弹射”吸附功能
      - 可吸附在墙体、窗框、车体上，不易察觉。
    - 虫戚：50年代苏联克格勃使用，火柴盒大小，可弹射



自然界依附贝类的寄生生物

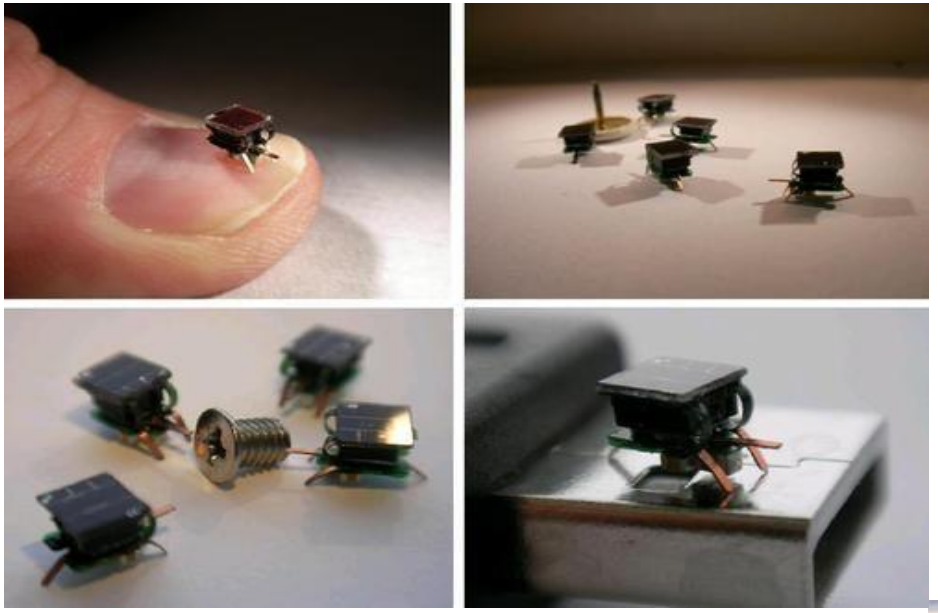
可弹射的虫戚窃听器

5.6.2 情报收集

- 2.窃听技术
  - 无线窃听
    - Kg和KgR：60年代克格勃使用
    - 体积：半英寸，方便藏进鞋底、桌角、烟灰缸、花瓶等

5.6.2 情报收集

- 2.窃听技术
  - 无线窃听
    - 苍蝇：60年代美国中情局使用
      - 体积：大头针大小，可来连续工作4小时。
      - 装在苍蝇的背上，通过门孔或通风口飞入房间进行窃听。



5.6.2 情报收集

- 2.窃听技术
  - 无线窃听
    - 独角仙：美国中情局研制
    - 体积小，能辩音、录音；适合嘈杂环境的窃听。

VS

5.6.2 情报收集

- 2.窃听技术
  - 无线窃听

电源开关窃听器　　VS　　玩具饰品窃听器

5.6.2 情报收集

- 2.窃听技术
  - 无线窃听

书脊窃听器

VS

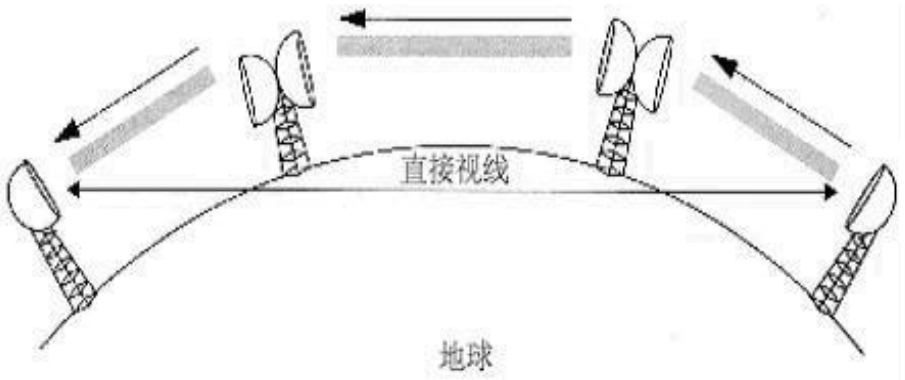
水泥地板窃听器

5.6.2 情报收集

- 2.窃听技术
  - 微波窃听
    - 微波窃听实质上也是一种无线窃听。
  - 原理：
    - 利用人们谈话的声波引起屋子里的窗户玻璃振动，在室外向窗户玻璃进行定向微波辐射，用高灵敏度接收机接收反射回来的微波，通过调制解调、分离这些微波携带回来的声波，并复原成声音。
  - 案例
    - **1976年莫斯科微波事件：美国大使馆发现几束强力微波从3个方面直射，微波辐射能量密度连续剂量最高达到每平方厘米180毫瓦(人体安全剂量不得超过每平方厘米10毫瓦)**

5.6.2 情报收集

- 2.窃听技术
  - 微波窃听
    - 微波电话窃听：微波通信，通过微波传递电话的声波。
      - 微波电话比有线电话更容易被窃听。微波电话需要在建筑物顶架设中继站，以接力的方式进行传输。
      - 长距离的微波传送，在中继的楔形地带，只要有相应的接收设备就能收到微波通信的信号，就如我们收听广播一样。
      - **1977.10**美苏上午谈判窃听



两个地面站之间的直接视线传输

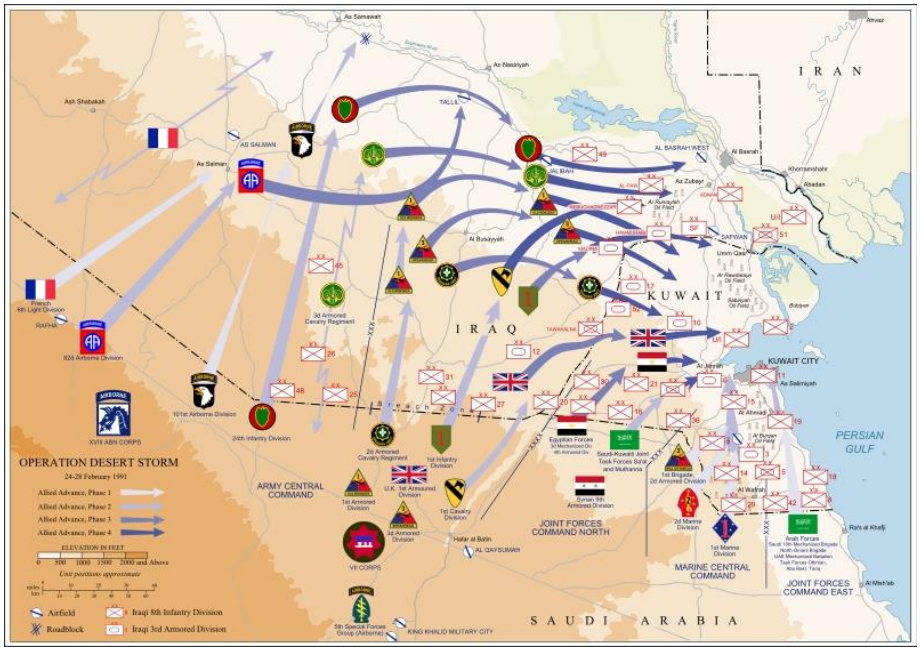
5.6.2 情报收集

- 2.窃听技术
  - 激光窃听
  - 原理：与微波窃听相似
    - 利用人们谈话的声波引起屋子里的窗户玻璃振动，在室外向窗户玻璃发射激光，用激光接收器接收玻璃反射回来的激光，通过光波分检处理，并还原成声音。
    - 优点：无需进入房间安装窃听器，避免了一旦发现被抓住把柄的危险。
    - 缺点：激光本身有局限，应用不广泛，无法替代其他技术。

5.6.2 情报收集

- 2.窃听技术
  - 激光窃听-案例

激光窃听设备

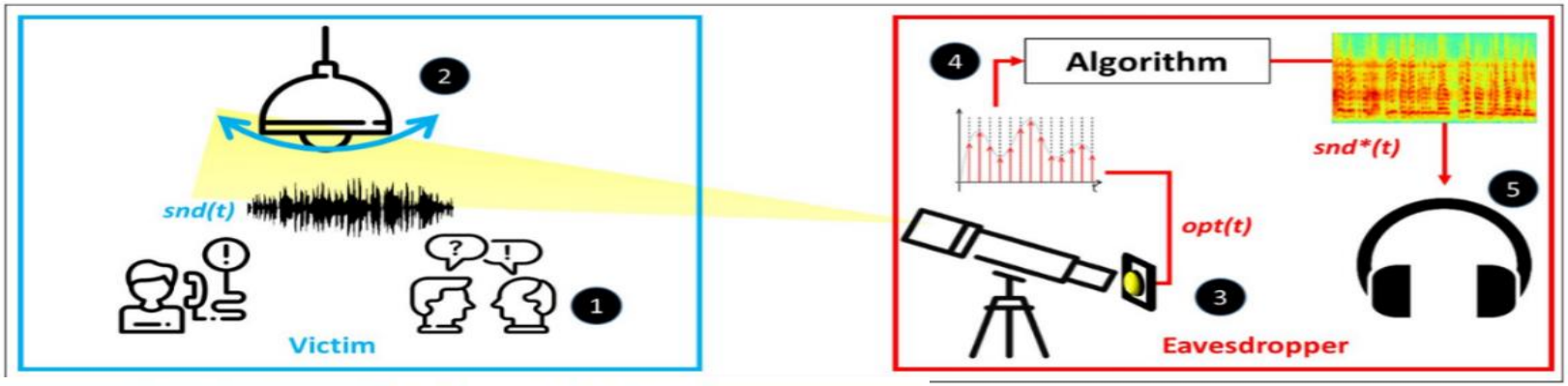


海湾战争：美国窃听

激光照射高级将领的汽车反光镜

5.6.2 情报收集

- 2.窃听技术
  - 激光窃听-案例(普光窃听)
    - 电灯泡+望远镜窃听器（距离25M）



5.6.2 情报收集

- 2.窃听技术
  - 影像设备窃听
    - 定向麦克风窃听
      - 高灵敏度的强方向性的麦克风，可有效地抑制干扰。
      - 能够窃听几米甚至几百米开外的谈话。在夜深人静的时候甚至可以窃听几公里远的地方。
    - 耳机窃听
      - 隔墙有“耳”窃听器：高灵敏度的音频放大器
      - 安装在一个房间的外墙侧，可穿透一米厚的水泥墙。

5.6.2 情报收集

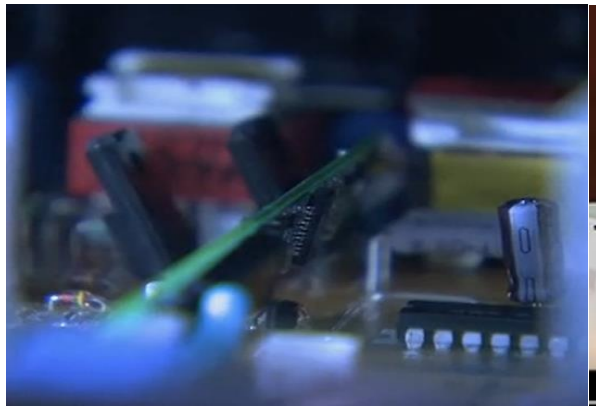
- 2.窃听技术
  - 影像设备窃听
    - 电视机顶盒(内嵌窃听器)

5.6.2 情报收集

- 2.窃听技术
  - 办公设备窃听
    - 打字机：内装微型窃听装置
      - 窃听使馆秘书打印的文件内容，并把它们发给藏在使馆墙壁里的收发信机，再把信号发给使馆外的监听站。
      - 1982年苏联人使用

5.6.2 情报收集

- 2.窃听技术
  - 办公设备窃听(现代办公设备安装数据窃听器)
    - 现代液晶多显示器的无线连接、有线连接
      - Win7-10的多显示器内容分享连接器
      - 电磁控制
    - 现代数字设备：办公用品，多功能一体机（电话、传真、复印、扫描）
      - 隐藏着秘密：可同时接受传真的秘密文件(《密战》)



5.6.2 情报收集

- 2.窃听技术
  - 办公设备窃听—外设窃听
    - 现代数字设备：手机、平板、笔记本电脑
    - 空调、复印机、打印机窃听

5.6.2 情报收集

- 2.窃听技术
  - 办公设备窃听--WiFi窃听
  - 窃听链接WiFi的任何设备
    - WPA2是用于保护现代Wi-Fi网络的安全协议。
      - Wi-Fi安全漏洞源于安全标准本身，而非个体设备问题，但它会影响到连接到Wi-Fi网络的设备。
    - CableTap攻击链：无线窃听用户的家庭网络
    - 免费wifi链接：可能导致用户手机被窃听
    - 公共WiFi攻击：内网监听攻击、伪造WiFi攻击。
      - 共同网络内窃取他人上网的内容：网盘上传的照片、微博
    - 伪造WiFi攻击：另一处同名的wifi链接
  - 防御
    - 设置复杂的密码；更改路由器密码
    - 隐藏SSID、关闭DHCP、绑定MAC地址、人走关闭电源

5.6.2 情报收集

- 2.窃听技术
  - 办公设备窃听----手机窃听
  - 手机是最好的追踪和泄密来源
  - 手机窃听技术
    - 手机卧底软件、蓝牙开关、免费WiFi
    - 伪基站窃听、安装微型窃听器、SIM卡被复制
    - 恶意手机USB充电线、充电器

5.6.2 情报收集

- 2.窃听技术
  - 办公设备窃听----手机窃听
    - 手机情报
      - 新手机在注册入网时实名制；
      - 设备ID和电话号码与个人信息绑定；
      - 手机在任何地方都会自动搜索基站，基站可以定位；
      - 手机wifi功能打开后也会自动搜索，wifi可以定位；
      - 手机黑屏假关机、应用卡顿、按键显示延迟（木马）；
      - 带SIM卡手机更容易定位；
      - 通话链接协议导致自动监听或录音通话内容；
      - 手机号码与邮件账户、购物账户、金融账户、通信账户绑定，容易遭黑客入侵。

5.6.2 情报收集

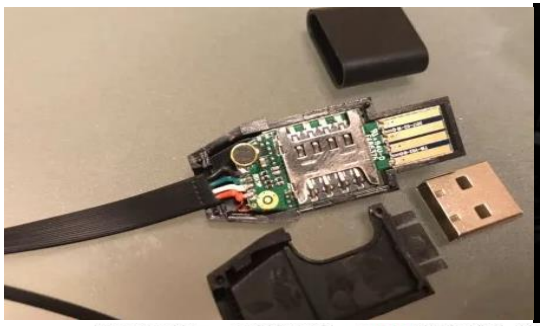
- 2.窃听技术
  - 手机窃听-八种主要途径
    - 01 基于物理/硬件的窃听
      - 手机里植入一个跟踪芯片，基于Nano SIM卡
    - 02 基于伪基站的窃听
      - 恶意干扰附近的基站，将该区域内的手机通信强制降级到2G(GSM-存在单向认证机制的缺陷)
      - 对手机通信实时解码监听：从短信到语音，再到通话内容
    - 03 基于应用APP的窃听
      - 商业间谍/监听APP：查看手机拨打电话记录，支持电话后台录音；支持监控社交软件聊天如微信、QQ。
      - 植入：WiFi热点植入、伪造短信或邮件、二维码下载、借用手机浏览特定页面。
    - 04 基于OS底层/驱动的窃听(少见)

5.6.2 情报收集

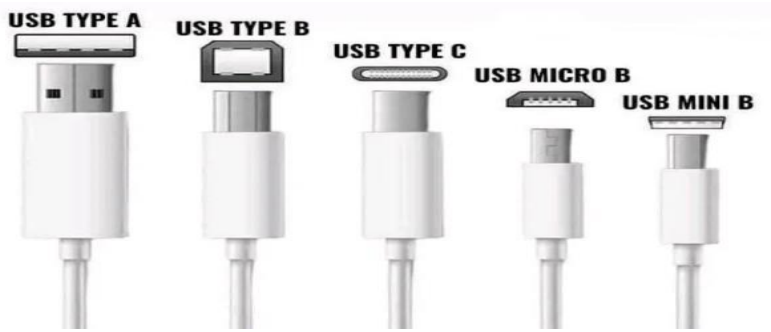
- 2.窃听技术
  - 手机窃听-八种主要途径
    - 05 基于手机漏洞的窃听
      - 安装特殊程序Hook系统shutdown方法，实现关机拦截，使手机处于“假关机”状态。
    - 06 基于手机其它功能的窃听
      - APP利用手机内置的加速度传感器实现对用户语音的窃听，且准确率达到90%。
    - 07 手机厂商的高权限管控
      - 苹果厂商可远程控制iPhone手机的一些功能，不但可以随时监视用户的生活。
    - 08 基于手机附件的窃听
      - 充电头内置窃听器/偷拍器。

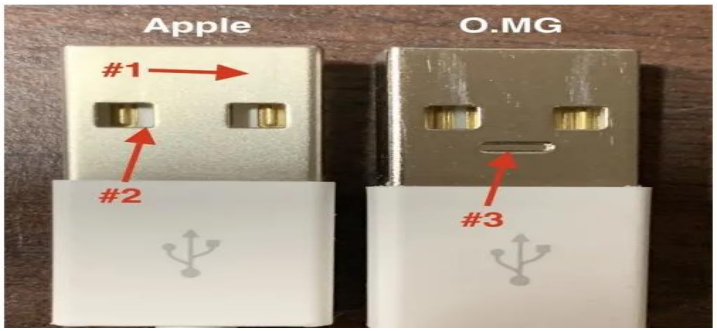
5.6.2 情报收集

- 2.窃听技术
  - – 手机窃听
    - 恶意手机USB充电线、充电器
      - – 功能：窃听（带SIM卡）、定位、植入木马、渗透内网



如下图所示，别的不说，USB充电线头若有右边这个类似"机器人笑脸"的外型，有问题的O.MG恶意充电线





5.6.2 情报收集

- 2.窃听技术
  - 手机窃听--应用APP窃听
    - 人脸数据窃取
      - 手机摄像头偷取个人人脸数据，用于商业情报间谍推理。
      - 潜在客户先逛A店，再进B店时，可通过人脸识别，并推断其购买意向。
    - 商业APP或游戏
      - 录制通话、收集短信和位置数据
      - 触发不良情绪的画面，都将被自动打码。
      - 被 APP 调取各种权限，可能购物时手机也悄悄在录音。
      - 商业的精准商品或服务推荐
      - 语音窃听与思想行为推理

5.6.2 情报收集

- 2.窃听技术
  - 手机窃听--应用APP窃听
    - 商业APP特点
      - 利益引诱下载 APP 并且给出系统权限
      - 或利用隐私策略的模糊二义性申明，引诱给出权限
      - 非法使用1-2周获取大量资金或信息后停用(如色情)
      - 合法窃取用户账号、密码、照片、微博内容、位置与行动路径等情报。
      - 控制用户行为：语音窃听与思想行为推理
      - 2021年以色列“飞马”间谍软件

5.6.2 情报收集

- 2.窃听技术
  - 手机窃听
    - 购物推荐、行为推荐、行为监控
      - 电影电视剧《窃听风云》《窃听风暴》
    - 思考
      - 你相信世间有灵异（鬼神仙）吗？
      - 你父母长辈相信吗？
      - 你曾亲历诡异事件吗？

5.6.2 情报收集

- 2.窃听技术
  - 反手机窃听--如何知道手机被窃听？
  - ①自我拨号验证法
    - 自己手机进行自拨，如果拨通或者告知为空号时，大概率被监听。
    - 措施：换电话卡（注销原有卡），把所有重要的app都换绑。
  - ②.通讯录检查法
    - 检查手机的通讯录，有不认识的“联系人”，不是自己添加的。
    - 措施：删除。如果删除不了就杀毒。
  - ③互证法
    - 通话时总是会莫名其妙挂断，如果询问对方没有操作，表示手机被监听了。
  - ④话费流量差异检查法
    - 仔细检查话费和流量账单，如果实际使用的和扣除的存在差异，基本表示手机被监听了。
    - 有人电话告诉你免费送语音、送流量、不明代缴话费很可疑。

5.6.2 情报收集

- 2.窃听技术
  - 反手机窃听--如何知道手机被窃听？
  - 5. APP管理检查法
    - 查看APP程序管理，如果发现未知或隐藏程序，很可能被监听了。
    - 措施：恢复出厂设置，更换APP。
  - 6.通话出现杂音、回音或干扰
  - 7.打电话总是需要2次才能正常接通
    - 第1次监听到，录音监听程序未启动准备；第2次才正常但录音了。
  - 8.频繁有骚扰电话或带链接短信
    - 骚扰电话购物优惠、确认链接；或随机发送红包优惠链接，其实是系统执行指令。
  - 9.手机总是异常发热，电池容易消耗。
  - 10.输入代码查看手机运作程序情况。
    - 输入*#*#4636#*#*或*#*#6130#*#*后点开使用情况统计，可查看一段时间的手机内应用使用情况，检查是否有异常程序运作。

5.6.2 情报收集

- 3.反窃听技术
  - 窃听设备的原理
    - 1） 通过声（光）波达到窃听的目的
    - 2） 电话窃听
    - 3） 手机窃听
  - 反窃听技术
    - 1） 防止激光射入房子窗户的玻璃：加层百叶窗；
    - 2） 破坏反射体随声音的正常振动：
      - 异型玻璃（厚斜）\音频噪声源贴在玻璃窗\室内播放录音或制造噪音。
    - 3）木马检查仪
    - 4）非线性节点探测器、手机探测器
    - 5）录音干扰器
    - 6）情报隐写、暗语

5.6.2 情报收集

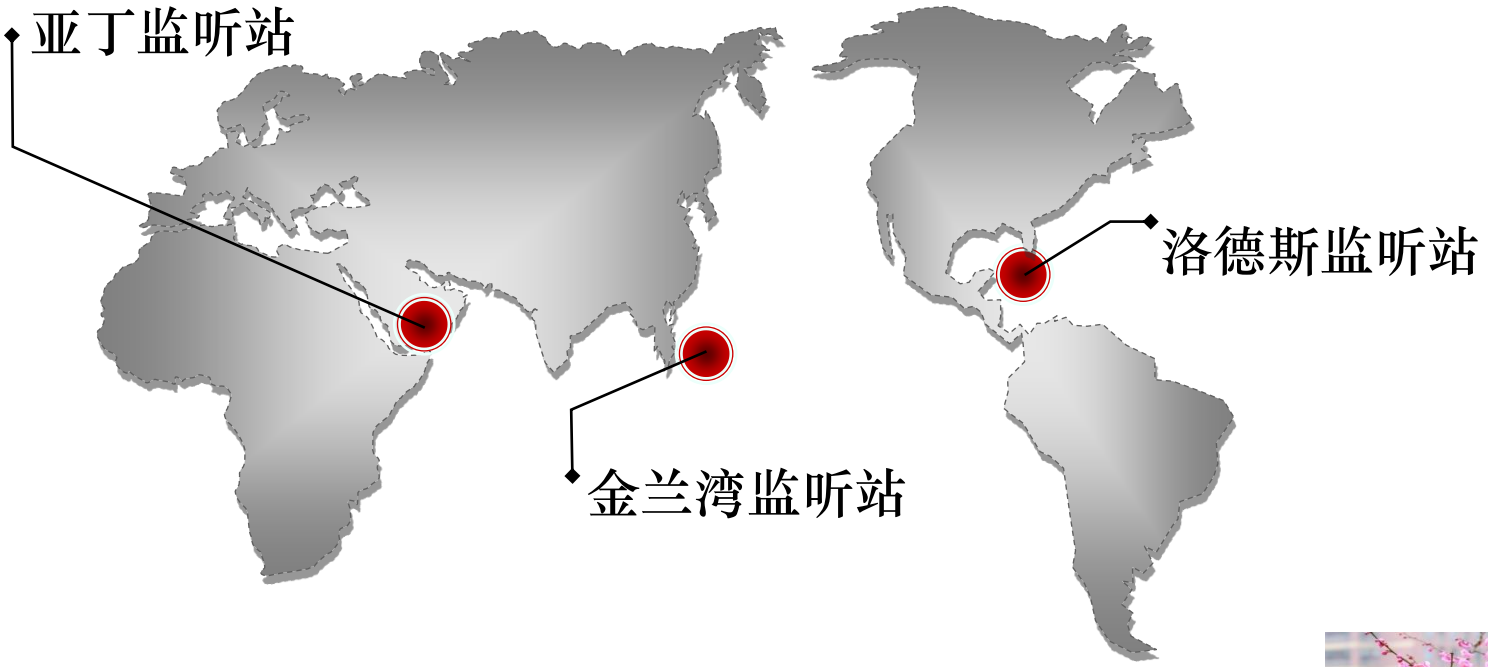
- 3.反窃听技术
  - 探窃器反窃听
    - 窃听器的发射机工作时会发出电磁波；
    - 探窃器灵敏度很高，可感应功率很小的发射机的电磁波。
    - **先进的反窃听器可感应窃听器的声波。**
    - **“频谱分析仪”、“场强测量器”**
      - **OSC-5000**相关频谱分析仪

5.6.2 情报收集

- 4.电子监听
  - 窃听只能用于近距离的目标，远距离的目标则要靠电子监听技术。
  - 电子监听又叫电信接收，指利用先进的电子设备系统对有线、无线、微波等通信信号进行截收、分析、破译、处理的全过程。
    - 电子监听仍属于一种电子侦察，实际上是窃听技术的综合发展。
    - 也是通信截收系统。

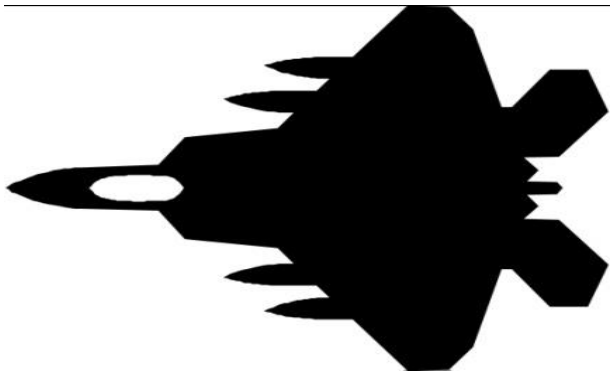
5.6.2 情报收集

- 4.电子监听
  - 苏联重要的地面监听站
    - 古巴哈瓦那的洛德斯监听站、在南也门的亚丁监听站和越南的金兰湾监听站。



5.6.2 情报收集

- 4.电子监听
  - 美国中情局的电子树枝
    - 1979年电子监听系统伪装成一段树枝，包上树皮，然后“嫁接”在紧靠苏联空军基地的一棵大树上。



5.6.2 情报收集

- 4.电子监听
  - 日本陆上自卫队电子截收站
    - 1987年防卫厅共有 9 个电子截收站，巨大的圆形天线群可截收来自任何一方的极其微弱的电波。
    - 收录军事通信，集中到东京的“别室”进行翻译和分析，汇总交到内阁官房长官。

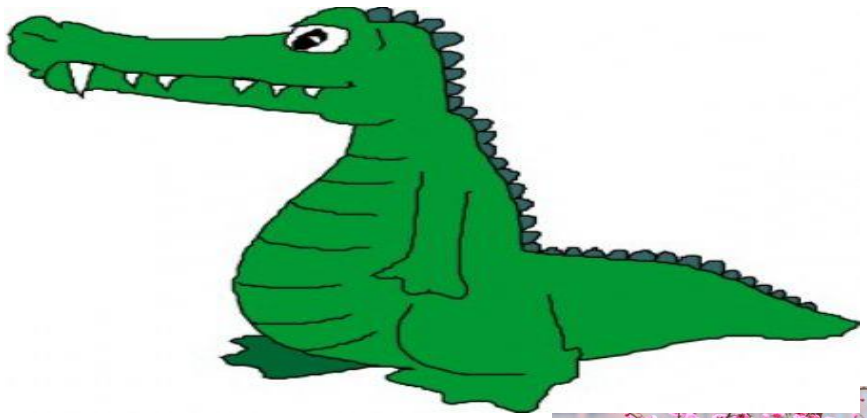
5.6.2 情报收集

- 5.窃照与窥视技术
  - 窃照和窥视是现代间谍窃密的重要技术手段。

窃照技术　　窥视技术　　窃照和窥视技术的应用

5.6.2 情报收集

- 5.窃照与窥视技术
  - 窃照技术
    - 是通过一系列的窃照器械来完成的。
    - 任何一个窃照器，实质就是一架微型化的照相机。
    - 用于军事、工业间谍
    - 各财团、企业均纷纷采用窃照技术，已泛滥成灾。
      - 美国“石膏大王”盖贝的礼物“鳄鱼标本”，眼睛安插着微型电视窥视录像机



5.6.2 情报收集

- 5.窃照与窥视技术
  - 窃照技术
    - 窃照装置多样化、微型化，五花八门
      - 藏进一块手表里、钥匙孔，显像装置不需要暗室
      - 《非常接触》中的90年代窃照设备

苏联克格勃研制的“FD-3”型微型照相机

美国1979年研制成功的手表照相机

联邦德国PK公司生产的“PK-420”型手表窃照机

日本登户研究所研制的“钥匙孔眼镜”

5.6.2 情报收集

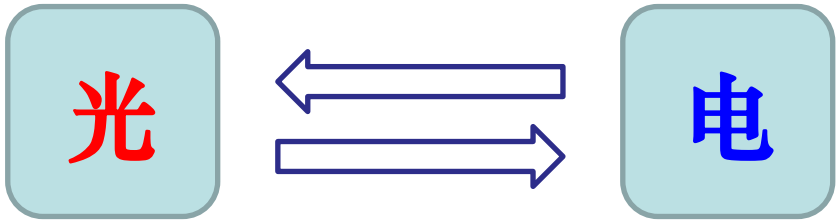
- 5.窃照与窥视技术
  - 窥视技术
    - 近代间谍窃密活动经常使用的一种有效手段。
      - 包括：探针、电视窥探、红外辐射、光纤技术、微光夜视

5.6.2 情报收集

- 5.窃照与窥视技术
  - 窥视技术
    - 探针系列
      - 探针内部装有光导纤维。可以透过针眼大小的微孔观察。伪装探孔很难被对方发现。可以窥视内部结构复杂、难以直接观察到的事物。
        - » 主要有KS-Q01、KS-Q02、KS-Q03等窥视器材
      - **KS-Q01**
        - » 最小的窥视器材，探针的直径只有**1.7**毫米。
      - **KS-Q02**
        - » 探头是一个光敏原件，与手柄之间是一条极易弯曲的软线。可与照相机、电视、电影设备连接使用。
      - **KS-Q03**
        - » 一种可伸缩的光学窥镜。物镜探头上有拉杆式天线，可伸缩调节，最大长度可达**800mm**。可窥视**暗处的物体**。

5.6.2 情报收集

- 5.窃照与窥视技术
  - 窥视技术
    - 电视窥视
      - 微型电视窥视录像机原理是光电转换，与普通电视类似。
      - 先把目标景象的光信号转换成电信号，再把这个电信号用有线电缆或无线电波传送到离景象很远的接收端，并在接收端监视器的屏幕上显示出来。
      - 与使用胶卷的微型照相机相比：无需胶卷、无需曝光，容量更大，只需藏在隐秘处，可录制屋内的一切情景。



5.6.2 情报收集

- 5.窃照与窥视技术
  - 窥视技术
    - 微光夜视
      - 把自然界微弱的月光、星光、大气晖光、银河光等照射下的目标反射回来的微弱光子借助于“光增大器”放大并转换为可见图像。
      - 微光电视录像机：微光夜视技术和电视技术相结合，能在非常微弱的光照条件下及时、连续的传送活动图像。

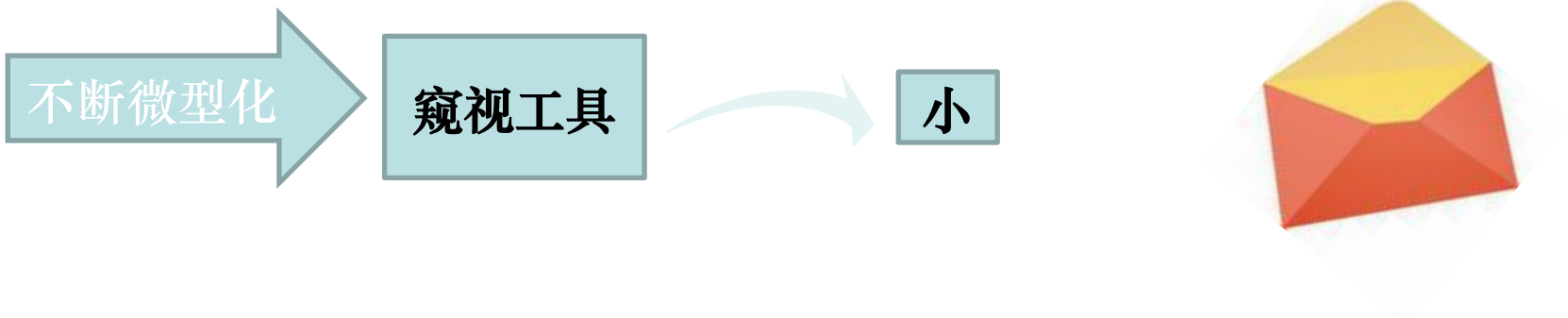
微光电视 < 普通电视

5.6.2 情报收集

- 5.窃照与窥视技术
  - 窥视技术
    - 光纤技术
      - 光纤+镜头：只需一束细软玻璃纤维作导线，沿着墙角一直拉到某个要窥视的房间，就可远程窥视。
      - PK-5060型光纤窥视系统
        - » 外径6毫米
        - » 长244毫米
        - » 窥视视角80度场景
        - » 视场距离>50毫米

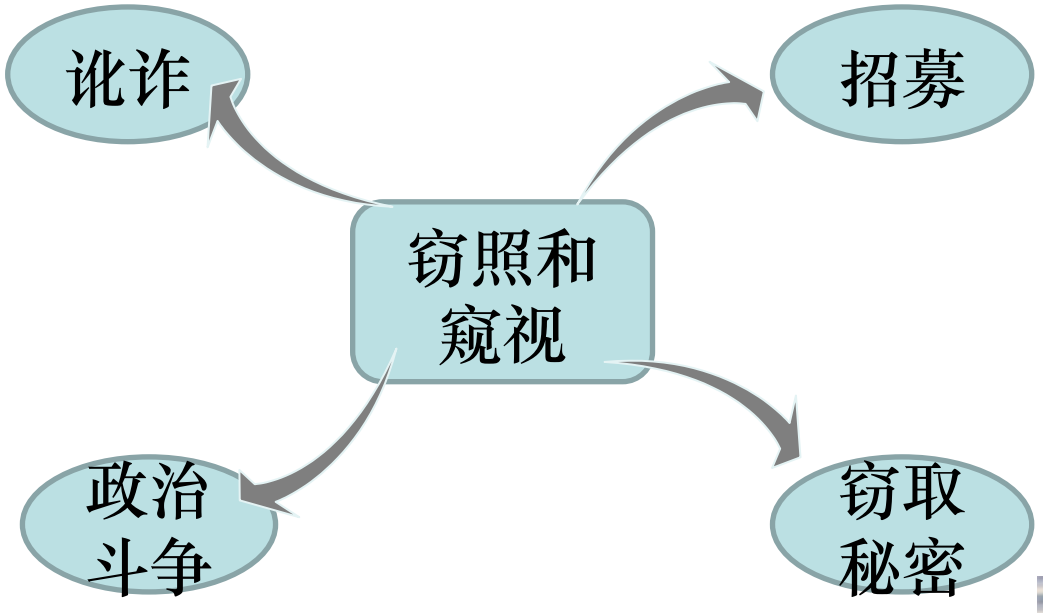
5.6.2 情报收集

- 5.窃照与窥视技术
  - 窥视技术
    - 红外辐射
      - 红外感应装置：可以把人体等热源物体发出的红外辐射光变成可以看得见的光。
      - 感应摄录距离：人体在30米内；运动物体大约150米。
        - » 微型针状灯：美国COS公司研制，专门用来窥视别人的信件。可以插进信封“读取”所需内容。



5.6.2 情报收集

- 5.窃照与窥视技术
  - 窃照与窥视技术应用
    - 间谍窃密的有效工具，情报机关广泛使用。
    - 安装：借维修改造房屋机会，在外国使馆安置。
    - 目的：

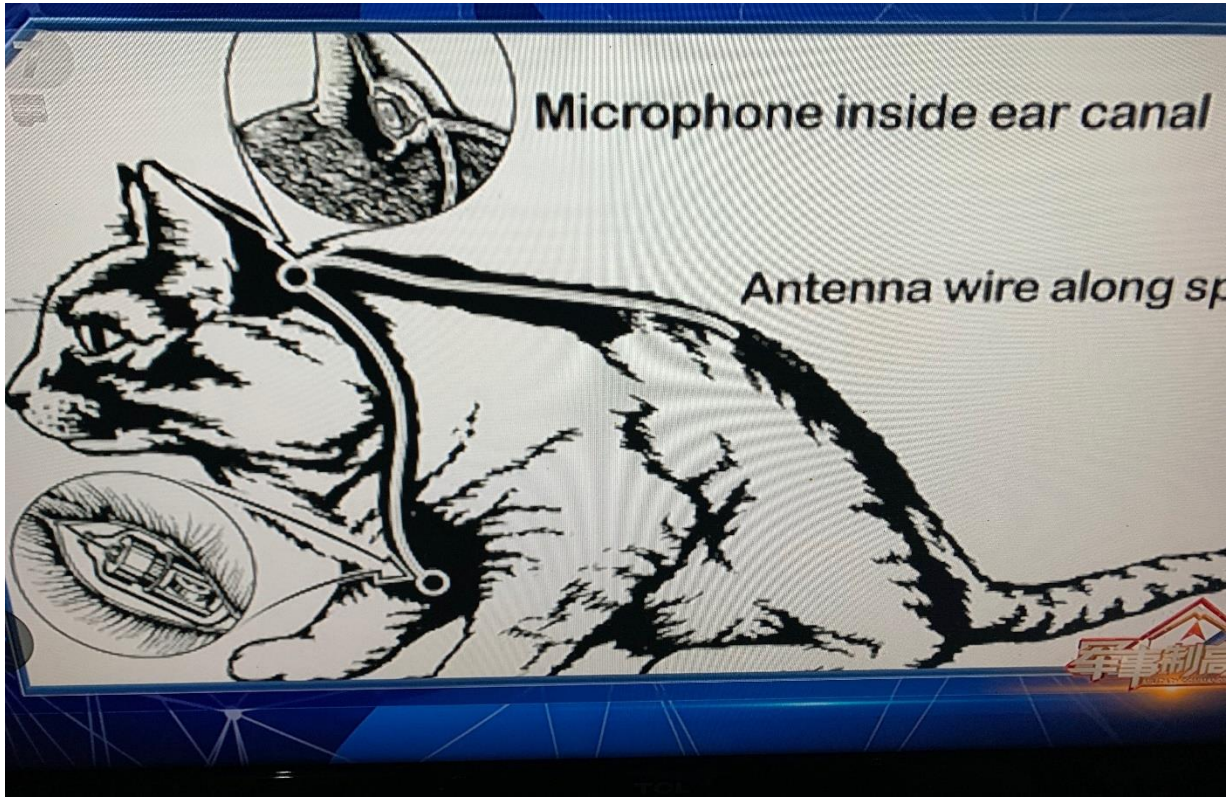


5.6.2 情报收集

- 6.电子监控与动物间谍
  - 海豚：捆绑电子声纳和微信相机

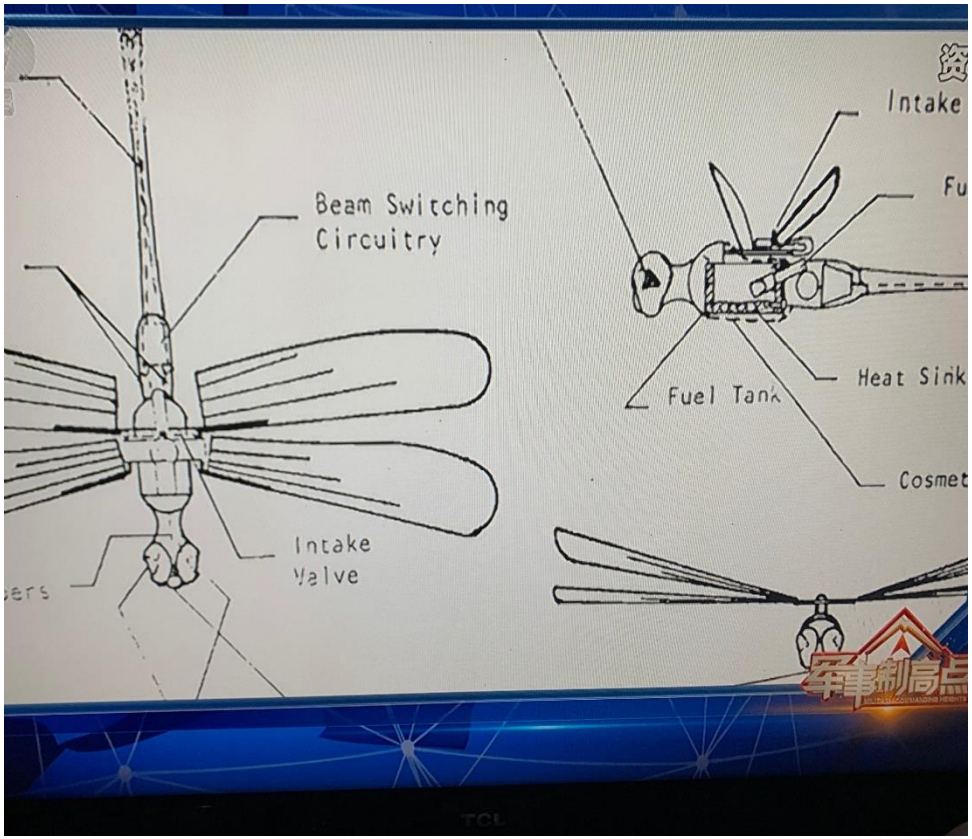
5.6.2 情报收集

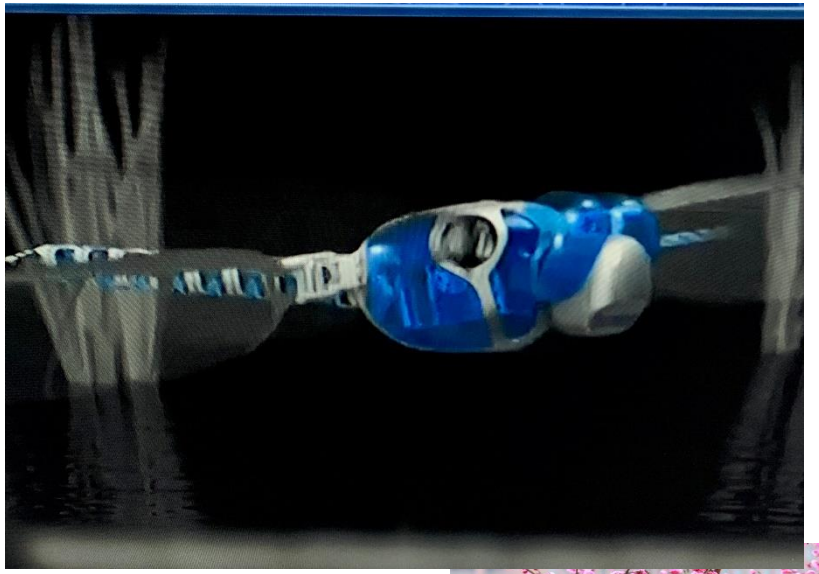
- 6.电子监控与动物间谍
  - 猫监听：方便跟踪、进入房间



5.6.2 情报收集

- **6.电子监控与动物间谍**
  - 仿生蜻蜓监控





5.6.2 情报收集

- 7.反窃照与窥视技术
  - 手机简单反红外窃照窥视
    - 将室内灯全部熄灭，拉上窗帘，使之成暗室；
    - 打开手机照相功能扫描室内，发现有红点，即有红外照相探头；
    - 手工清除。
  - 专业窃照探测器
    - 一般较贵
  - 参看电视剧《密战》

小结

- 人员管理是将合适的人员配备到合适的职位上，并让其从事合适的工作，从而实现“人适其位，位得其人”。
- 人员安全管理指与组织或企业的业务信息系统相关的人员的安全管理。
  - 人员分类：内部人员、准内部人员、特殊身份人员、外部人员(个人与小组)、竞争对手
- 人员安全管理原则：
  - 多人负责原则、任期有限原则、职责分离原则
- 企业人员安全管理措施包括
  - 领导者安全意识、系统管理员安全意识、一般用户安全意识、外部人员安全管理、内部人员安全管理
  - 重要的是内部人员的安全管理。
- 间谍的主要任务是采取非法或合法手段、通过秘密或公开途径窃取情报。

习 题

- **4.信息安全人员的审查应当从哪几个方面进行?**
- **5.人员安全管理的基本原则是什么?**
- **6.职员授权管理的主要内容有哪些?**
- **7.有哪些常见的物理失窃密技术?**
- **9.不考虑中继,窃听最远的是什么技术和设备?**