对物联网引发的安全问题的思考与对策

陆宝华

对物连网引发的安全问题的思考与对策

- 引言
- 物连网的构成
- 物连网各要素的脆弱性分析
- 物连网对国家安全的影响
- 物连网对社会公共安全的影响
- 对策

引言

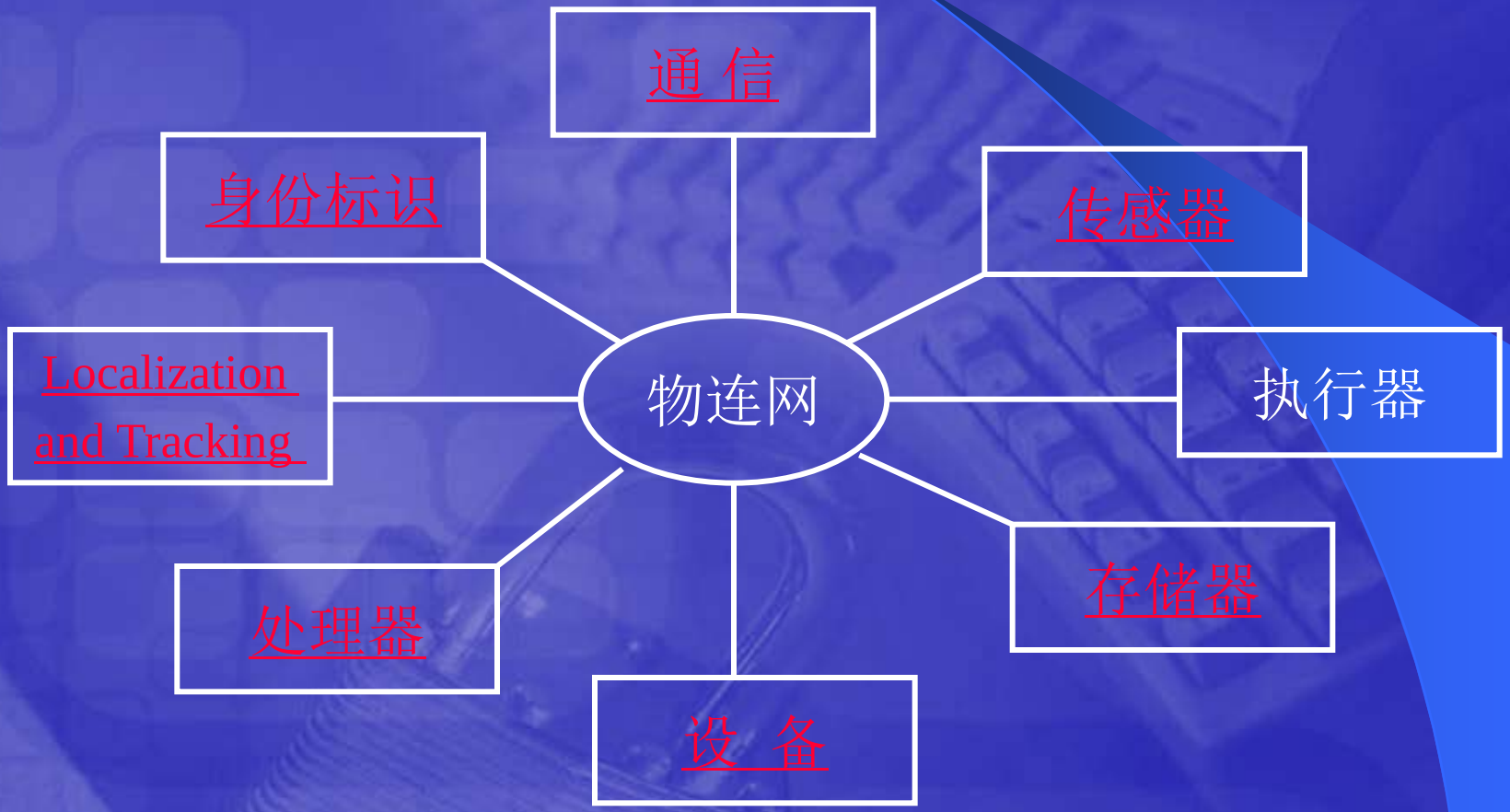
- 物连网美妙的前景
- 各厂商对物连网的热情
- 物连网可能会引发安全问题

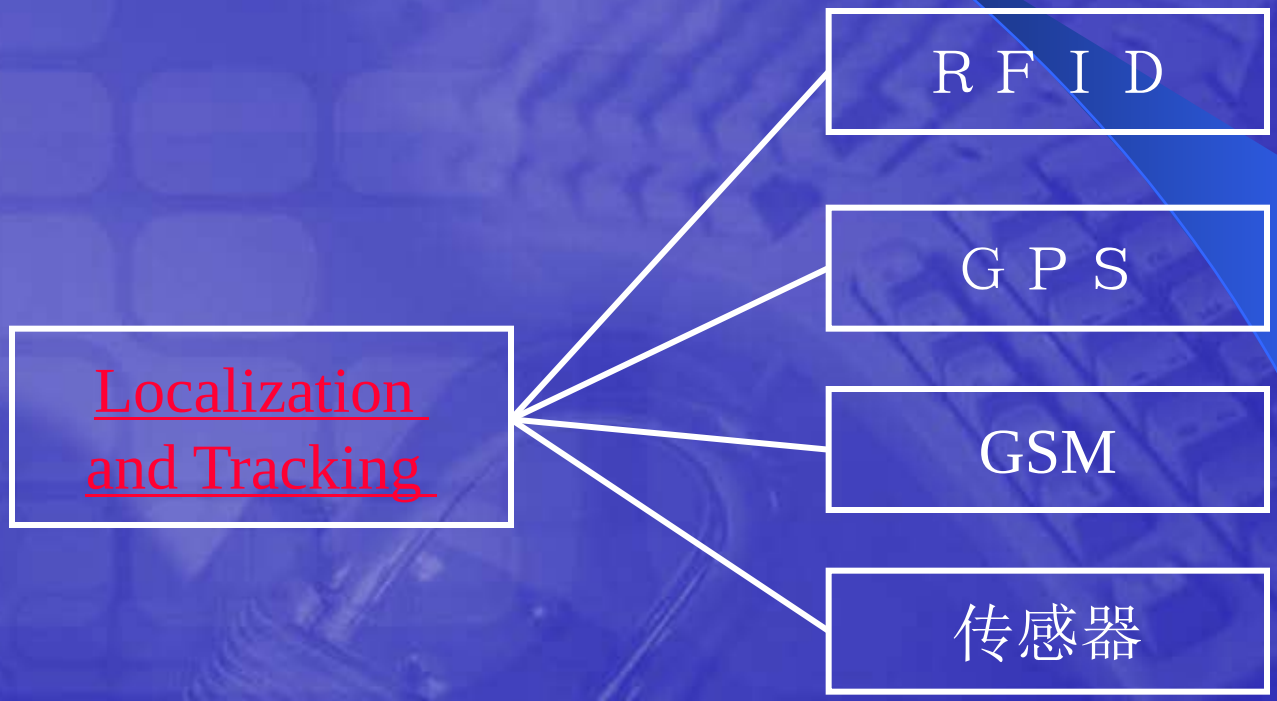
  1、物连网本身的安全问题

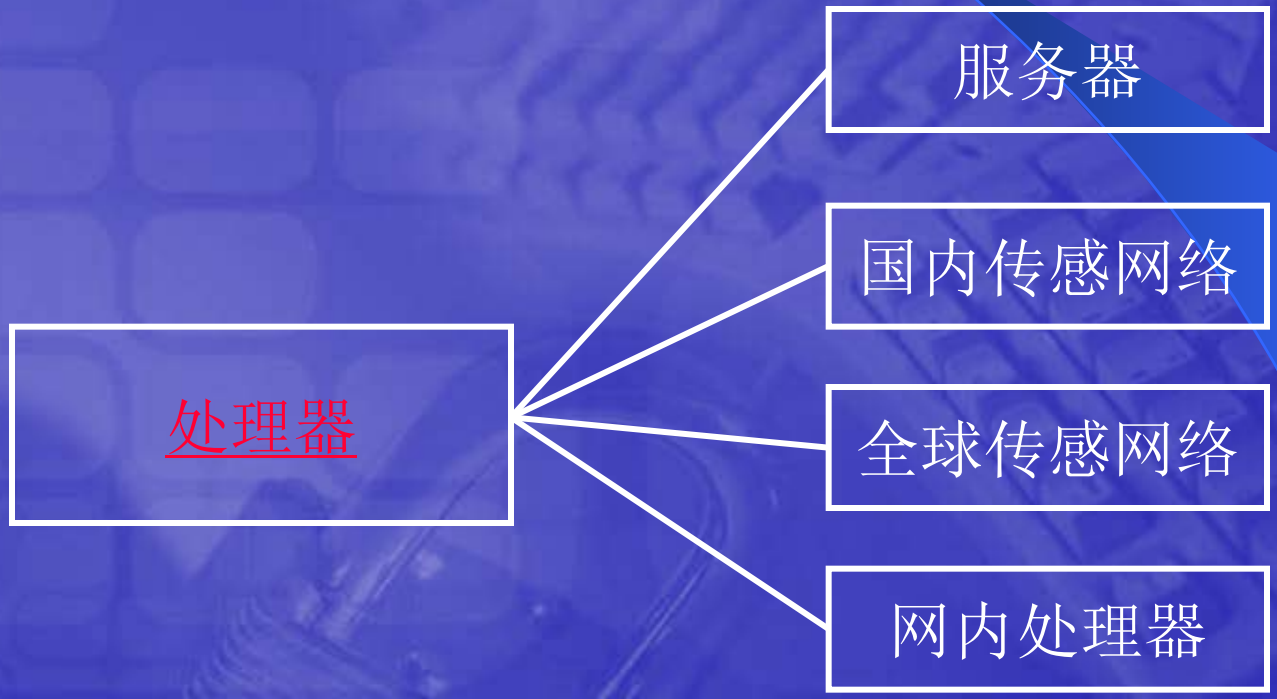
  2、物连网对国家安全产生重大影响

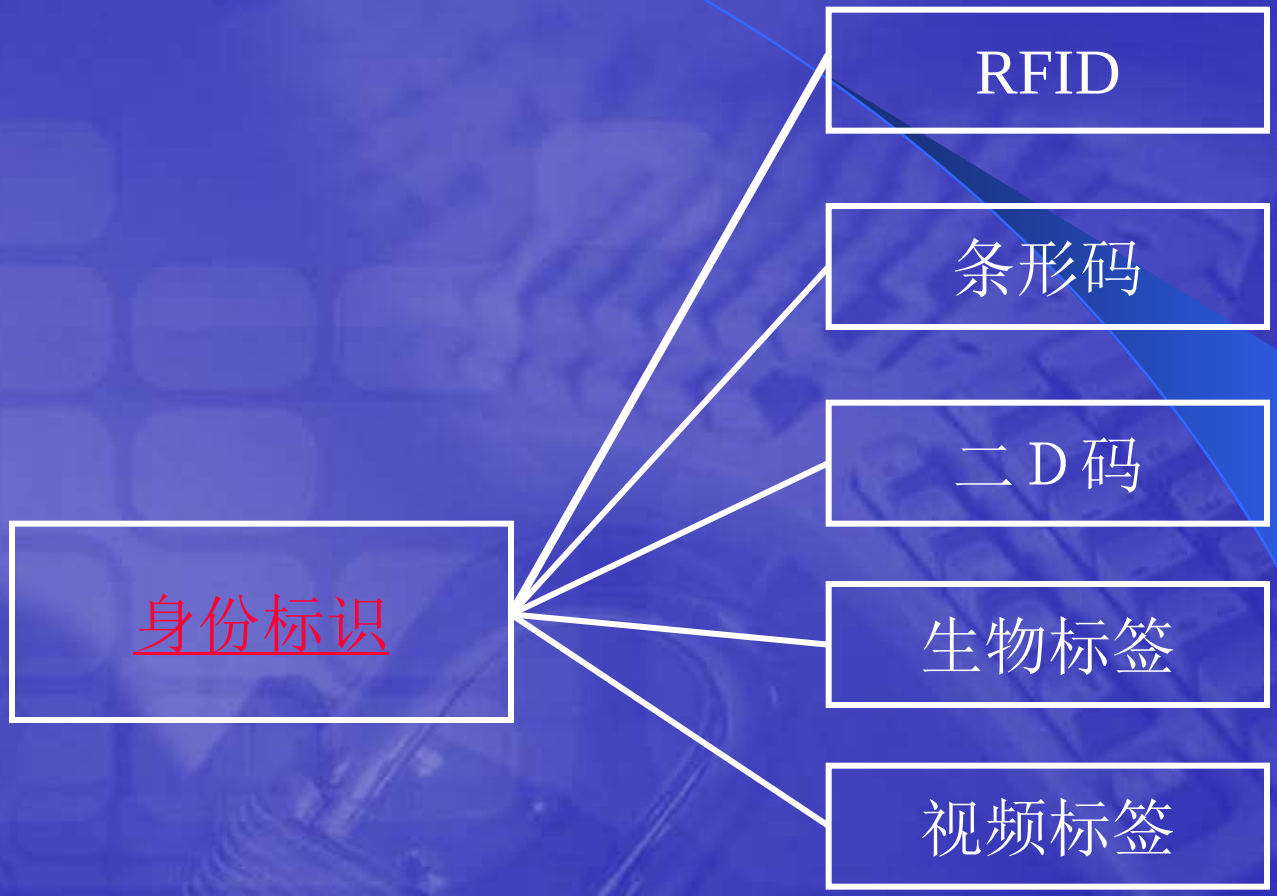
  3、物连网可能引发的社会安全问题

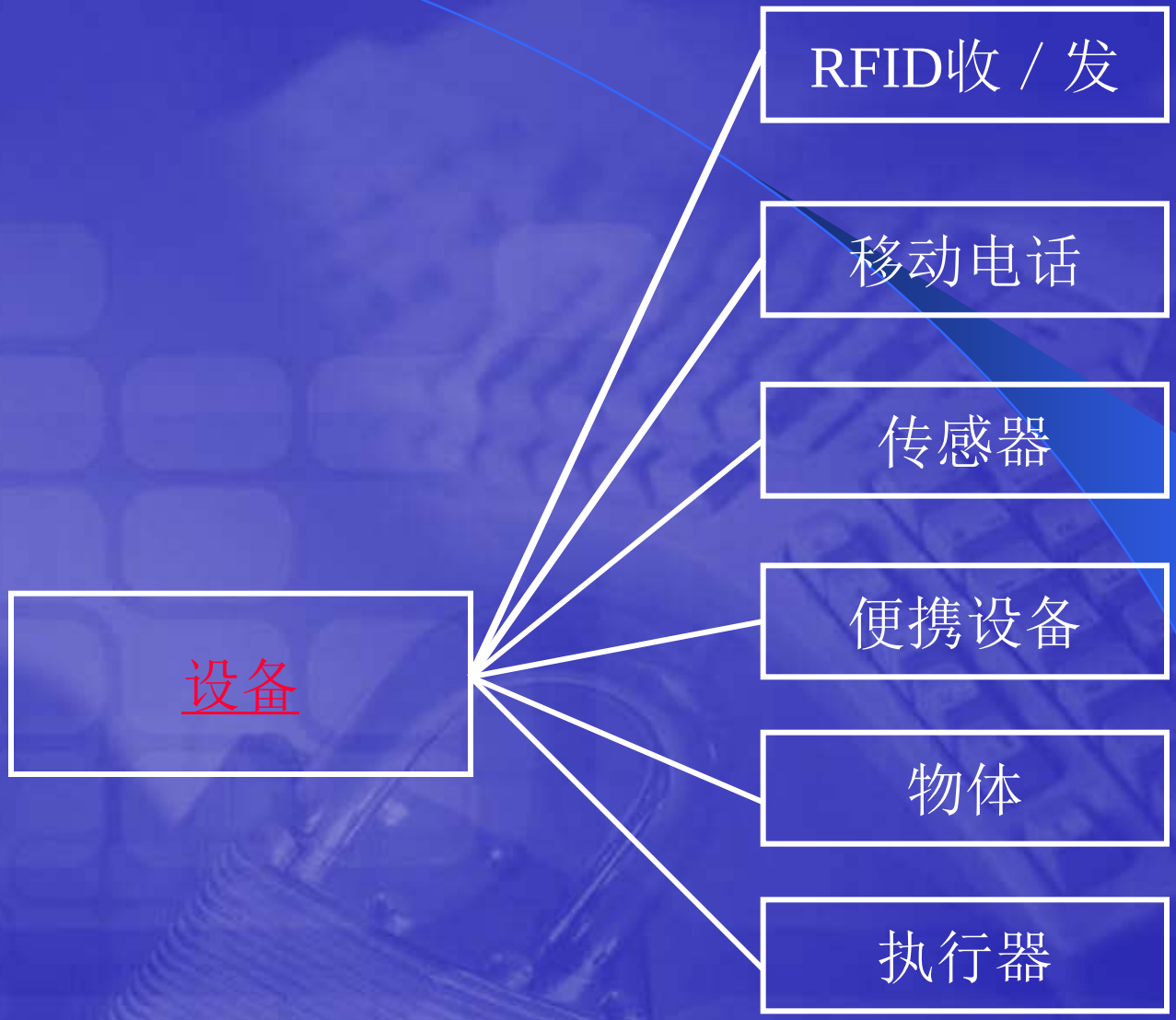
构成物连网的要素

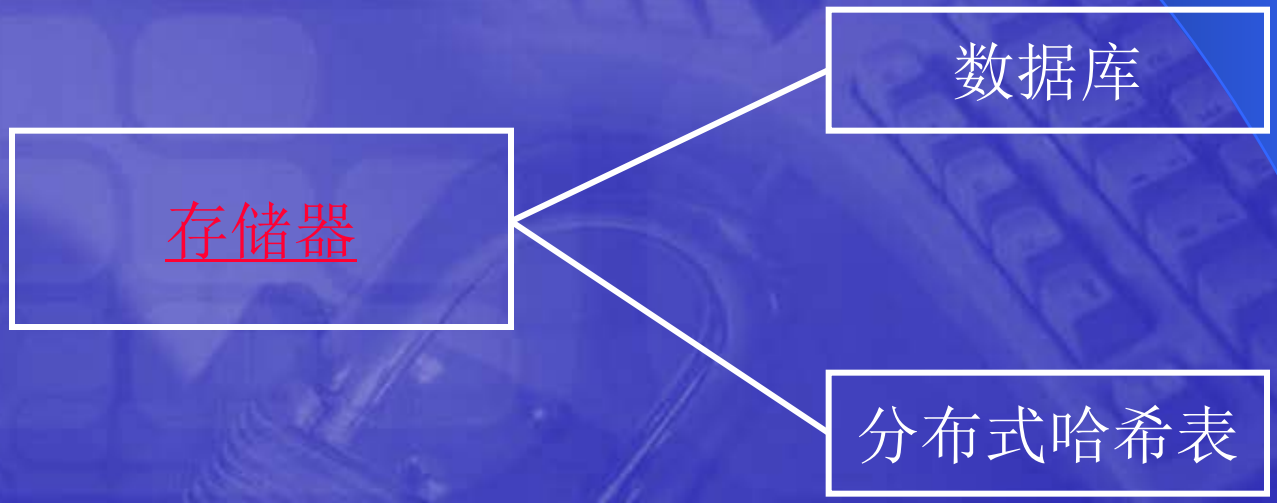


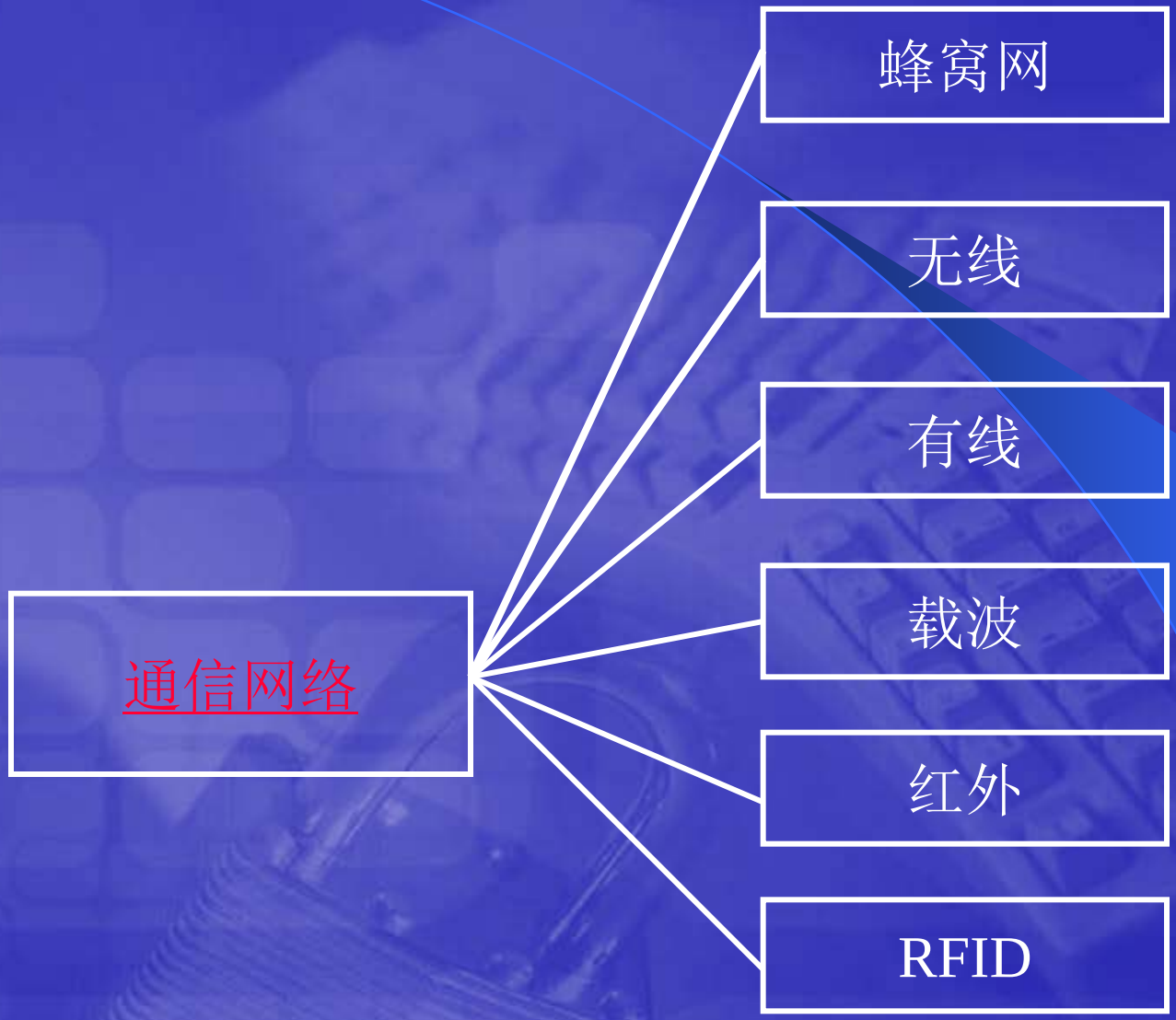

Localization and Tracking
RFID
GPS
GSM
传感器

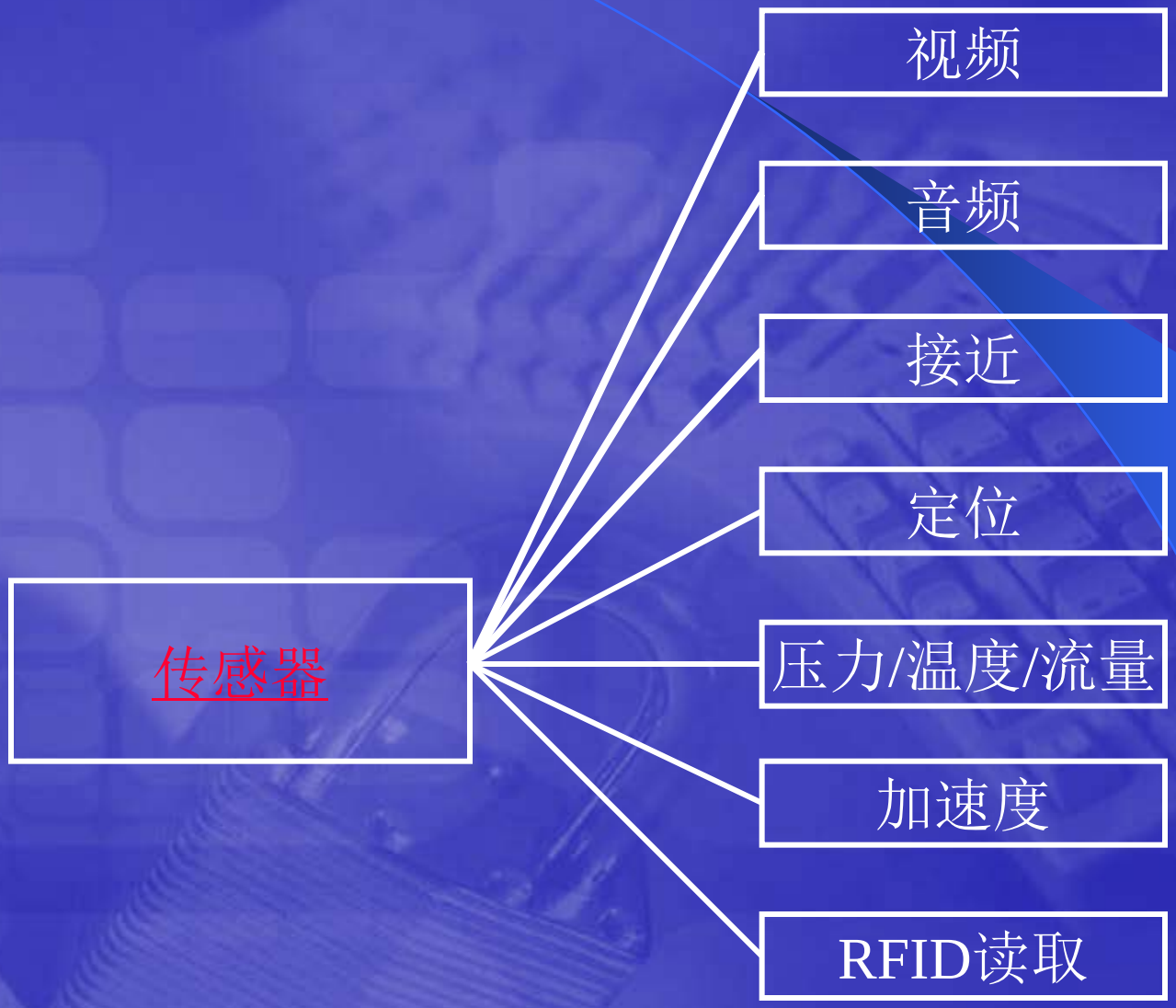

处理器
服务器
国内传感网络
全球传感网络
网内处理器


身份标识
RFID
条形码
二 D 码
生物标签
视频标签


设备
RFID收／发
移动电话
传感器
便携设备
物体
执行器


存储器
数据库
分布式哈希表


通信网络
蜂窝网
无线
有线
载波
红外
RFID

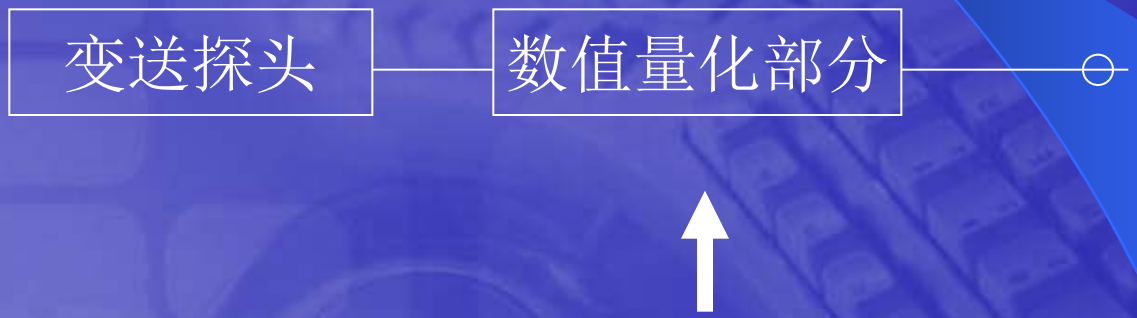

传感器
视频
音频
接近
定位
压力/温度/流量
加速度
RFID读取

构成物连网的要素

- 1、传感器及传感接入系统
- 2、地理信息
- 3、通信系统
- 4、ＲＦＩＤ等标识信息
- ５、基础网络（包括服务器及数据库等）

构成物连网要素的脆弱性分析

- 传感器



构成物连网要素的脆弱性分析

- 传感器接入

构成物连网要素的脆弱性分析

- 通信系统
- 对于有线：搭线窃听；光纤也可能用光纤三通进行分光。
- 对于无线：无线的泄露和插入是很容易的。
- ＣＤＭＡ虽然有一定的保密性，但不是可靠的。
- 载波也是可以泄露和插入的

构成物连网要素的脆弱性分析

- RFID
- RFID的数据是可以复制和伪造的
- RFID本身并具备物体的属性，物体属性是人为附加，并且在数据库中进行保存。
- 数据库是可能被侵入的，侵入后数据就可能被篡改
- RFID相当多数是无源的，很难将时间戳信息加入。

构成物连网要素的脆弱性分析

- ＧＰＳ
- 可能会泄露重要目标的地理坐标，包括固定目标和移动目标。如果是以军事为目的的目标，就可能成为被敌方打击的对象。或者进行伪造

构成物连网要素的脆弱性分析

- 高度的自动化
- 由于有执行器，系统可以实现高度的自动化，完全是由计算机控制相关的设备按相关程序完成操作。包括：交通工具的驾驶；医疗；生产的过程的各种环节；社会管理等等方面。
- 由于没有人的直接参与，存在的风险相当大。

构成物连网要素的脆弱性分析

- 基础信息网络存在的脆弱性
- 由于网络协议和主机操作系统存在的严重的脆弱性，网络攻击的风险是大量存在的，特别是将来的物连网与云计算相结合，云本身的安全问题将对物连网产生极大的影响。各类攻击事件现在每天都在发生。去年底的CSDN事件和Putty事件及前些年发生的各类病毒，和攻击事件都说明这一问题。

对国家安全的影响

- 网络战是目前全世界许多大国都在抓紧研究和带有战略性的部署，美国已经成立了网络战部队。但是基于计算机网络的网络战，除了对计算机网络目标能够直接打击外，多数情况下对于非计算机的网络目标还不能实施直接打击和破坏。在基于物连网环境下，网络战的直接打击目标绝不仅仅是计算机网络目标。各种视在目标也都可能是被打击的对象。

对国家安全的影响

- 美国对伊朗的离心机的破坏和伊朗诱落美国的无人机，都可以看成是网络战直接破坏非计算机网络目标的预演。而物连网建成后，这种打击的目标会变得更加广泛，手段也会是五花八门。如制造恐怖事件，破坏基础设施和工业设施，破坏交通运输等等。破坏电力设施。

对国家安全的影响

- 7.23涌温线的动车相撞是一起责任事故，这种责任事故会不会变成恐怖事件的翻版呢？。

对社会公共安全的影响

- 网络的发展，导致了利用网络进行犯罪，目前形形色色的网络案件频繁发生，几乎每天都各类的诈骗，盗窃等案件来报案。但是这些案件绝大多数是将网络作为通信或者媒体工具，除了对网上银行等金融系统可以实施直接的犯罪，而对于其他领域，网络仅仅是犯罪的间接手段。

对社会公共安全的影响

- 在物连网环境下，不仅网络遍布到各个角落，而且自动化程度会相当的高，整个社会似乎是在被机器控制和管理着。所以，笔者认为除了性侵害犯罪没有办法利用网络直接实施以外，其他的犯罪几乎都可以利用网络来直接实施。而且，由于是利用网络，使得面对面进行犯罪的心理障碍没有了，一些犯罪可能就像在玩游戏。

对社会公共安全的影响

- 制造杀人案件
- 制造爆炸
- 纵火等案件
- 盗窃资金
- 盗窃贵重物品
- ……

对经济的影响

- 物连网可能导致的安全事件对经济建设的影响，目前还无法做出科学的预测，但是可以肯定的说，一旦发生了恶性安全事件，对国家经济的打击肯定是巨大的。7·23，甬温线动车相撞事故后，国务院调查报告中给出的数据：“造成40人死亡、172人受伤，中断行车32小时35分，直接经济损失19371.65万元。”

对经济的影响

- 一些机构做了统计，下面这段文字是采用了网上的一个统计数据。
- “事故发生后高铁概念板块整体重挫，高铁指数下跌5.81%，33只高铁概念股(剔除停牌个股)总市值蒸发316亿元。尽管随后多家上市公司发布澄清公告，撇清与事故的关系，但仍然未能遏制整体颓势。不仅如此，在外媒对中国高铁也是一片"唱衰"，风头正劲的高铁出口前景也黯淡了。至于究竟本次事故会给中国经济发展造成多大的影响，还有待时间的检验。”

对经济的影响

- 如果在物连网环境下发生了网络战，银行的信息系统被摧毁，或者资金安全发生了问题；
- 或者对一个国家的基础设施、工业设施进行摧毁性打击；
- 或者…
- 那么对一个国家的经济的影响将是很难估计的。
- 7.23涌温线动车相撞事故，和上海地铁列车追尾事故，已经在给我们报警了；同样，伊朗将美国的无人机诱捕也是基于物连网的战术。

物连网肯定会给人类带来巨大的利益，所以不能因噎废食。但是，如果不能对可能产生的风险及早进行研究并拿出相应的对策，那么后果也将是可怕的。

对策

- 加强信息保障，提升目前的整体的安全水平，特别是要害部位的信息保障水平。特别是应该从网络和主机操作系统两个方面提升信息保障的水平。云计算一定要有我国自主知识产权的Hypervisor
- 建议建立全国性的网络犯罪监控、防范与取证体系。

对策

- 1、首先建立全国性的网络犯罪监控、防范与取证体系。
- 这个体系应该是一个全球黑客定位、黑客分类和分级、黑客跟踪、黑客行为分析、取证系统。应致力于跟踪分析全世界范围内的黑客攻击行为及事件，整合成一个集黑客信息、攻击行为、攻击方式、捕获到的0day等信息为一体的数据库，并以此为更多产品及服务提供云端数据接口、报表以及参考依据。

对策

- 反恐对任何一个国家都是一个巨大的挑战，因为一直以来我们都无法知晓恐怖分子带着何种目的从哪里来？何时来？使用什么武器？目标是谁？我们在面对互联网黑客和恐怖分子时也是一片茫然，面临同样的挑战！而在物连网环境下，这种挑战还会更复杂。难度为更高，更需要这种全国性的监控系统。
- 通过对黑客的行为及行动轨迹分析，我们可以清楚的知道：

对策

- 黑客从哪里来
- 到哪里去
- 做了什么
- 用什么工具和手段
- 攻击结果如何
- 真正做到全方位跟踪任意黑客的攻击行为，分析其特征及目的。
- 建立这样体系，就需要在重要的网络节点，国际出口，及重要的接入网络边界安装相应的监控工具，并且建立集中的监控中心。通过对即时的和历史的数据关联，不同地域的同类行为关联等，进行安全事件的预警、防范、和取证。

对策

- 2、应该加强基于物连网环境的取证技术研究
- 目前基于互联网环境的取证技术研究，已经取得了一定的成就，通过对审计技术、IDS技术、报文分析技术、IP确认技术、路由信息分析、多媒体数据分析、存储介质分析、数据分析等，可以对部分信息安全事件的认定、形成有效的证据链。
- 在物连网环境下，仅有目前水平的取证技术研究是远远不够的，还需要对物连网的一些特殊环节的取证技术进行研究，如：传感器数据的审计、RFID与地理坐标信息的轨迹分析技术、传输通道中的异常数据流分析等。

对策

- 3、电子证据与现实社会中的证据关联技术研究
- 物连网是将传统社会向网络社会转移，利用物连网实施的犯罪，也必然会有现实社会中的痕迹，在形成证据链时，也不忽略现实社会中的痕迹。应该将现实社会中的行为痕迹与电子证据之间进行关联。

谢谢！