陈晓桦

标准化基础知识

中国信息安全认证中心
China information security certification center

报 告 提 纲

1. 标 准 化
2. 标 准
3. 标准化文件
4. 标准在规范性文件体系中的地位
5. 标准化的作用及效益

1 标准化

活动

标准化 standardization

为了在既定范围内获得最佳秩序，促进共同效益，对现实问题或潜在问题确立共同使用和重复使用的条款，编制、发布和应用文件的活动。

注1：标准化活动确立的条款，可形成标准化文件，包括标准和其他标准化文件。

注2：标准化的主要效益在于为了产品、过程和服务的预期目的改进它们的适用性，促进贸易、交流以及技术合作。

目的

范围

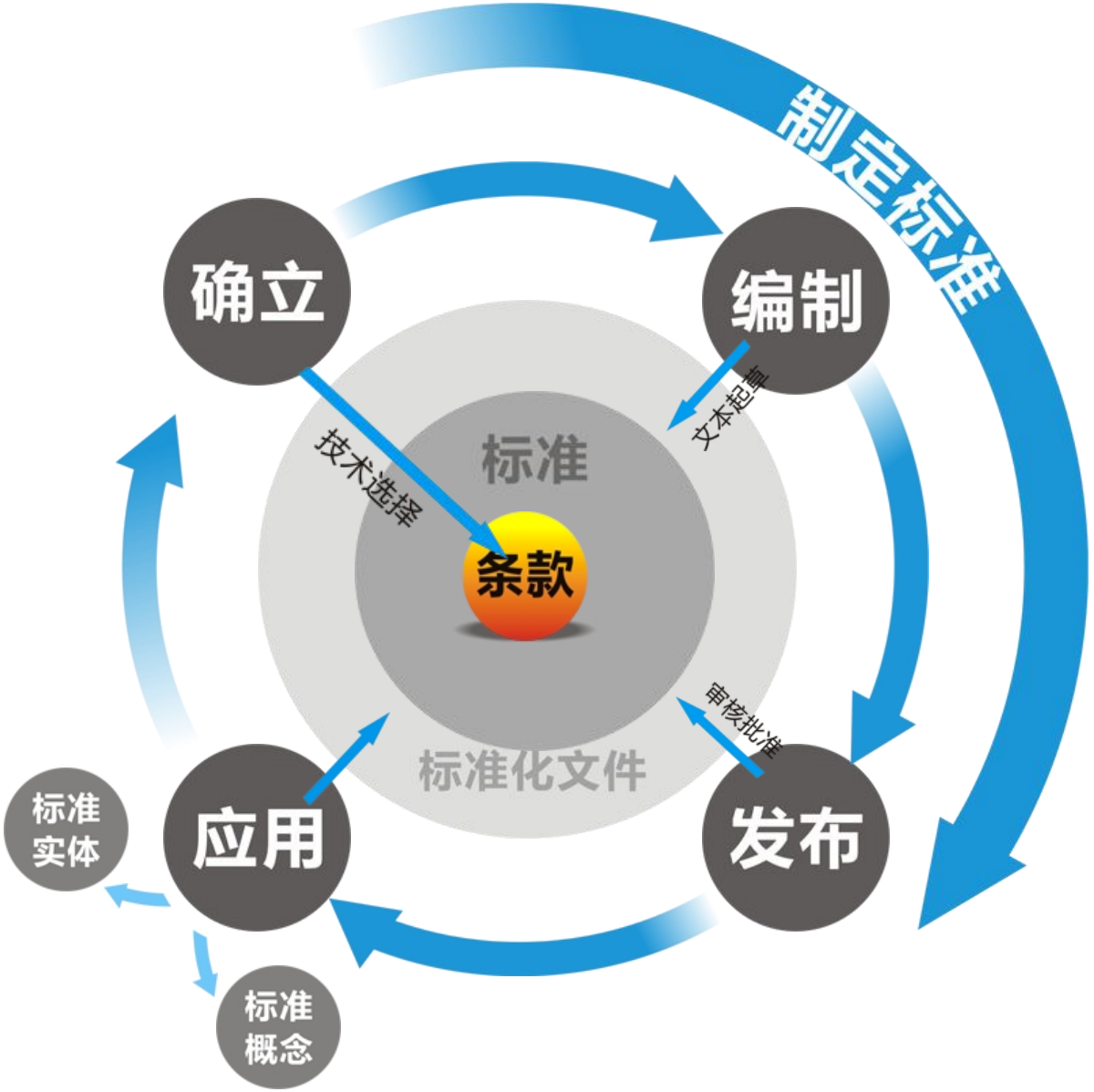
对象

内容

产出

效益

1 标准化 - 活动内容



2 标准

文件

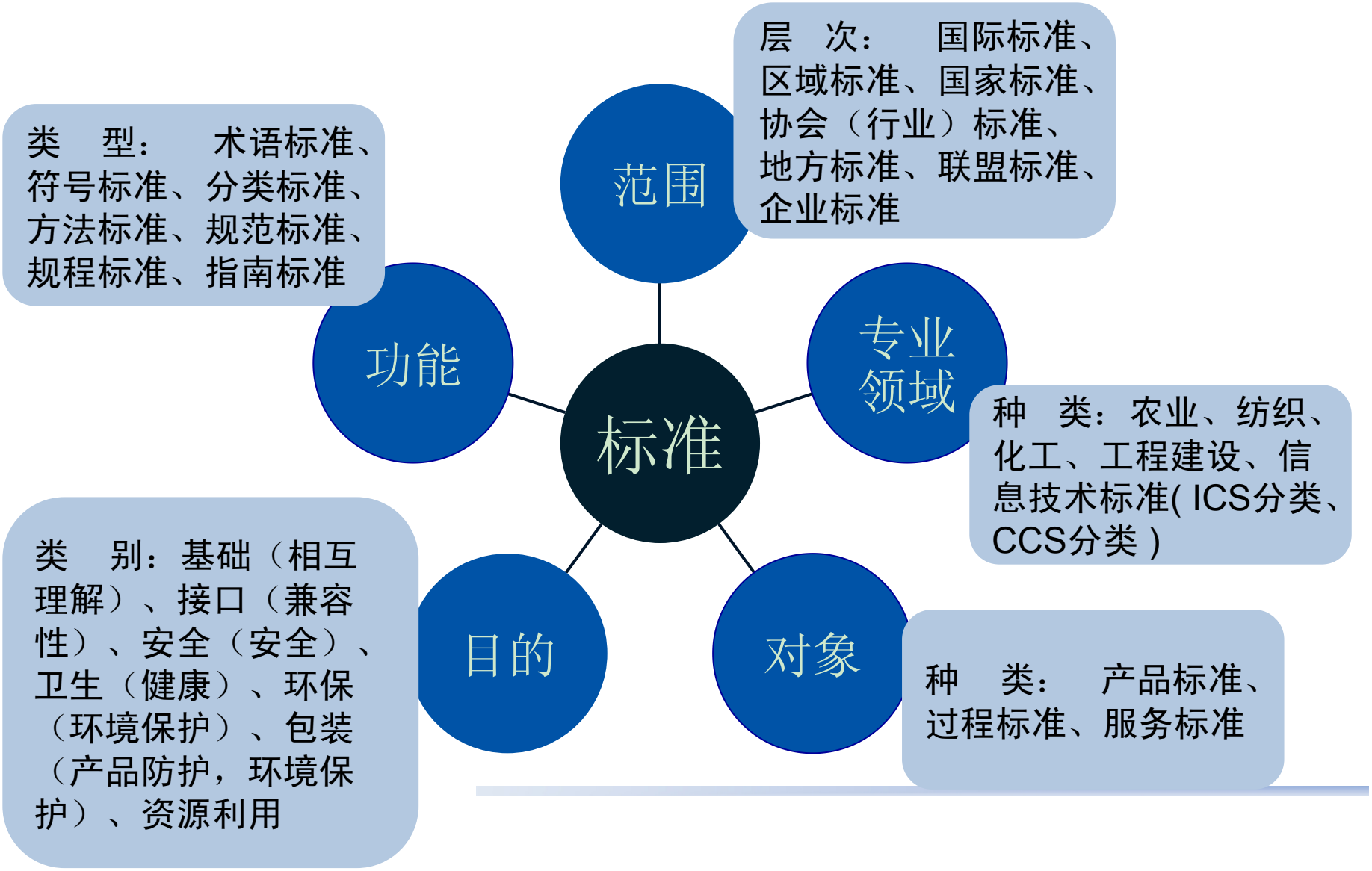
标准 standard

通过标准化活动，按照规定的程序制定，为各种活动或其结果提供规则、指南或特性，供共同使用和重复使用的文件。

注：标准宜以科学、技术和经验的综合成果为基础。

- 形成
- 功能
- 特点
- 基础
- 形式

2 标准-分类


标准
范围
层　次：　国际标准、区域标准、国家标准、协会（行业）标准、地方标准、联盟标准、企业标准
功能
类　型：　术语标准、符号标准、分类标准、方法标准、规范标准、规程标准、指南标准
专业领域
种　类：农业、纺织、化工、工程建设、信息技术标准(ICS分类、CCS分类)
目的
类　别：基础（相互理解）、接口（兼容性）、安全（安全）、卫生（健康）、环保（环境保护）、包装（产品防护，环境保护）、资源利用
对象
种　类：　产品标准、过程标准、服务标准

2 标准-分类

- 标准属性

  GB/T 14784-1993《带式输送机安全规范》，ICS号为：53.040.10，CCS号为：J81
- 层次：国家标准
- 标准的种类为机械产品标准
  - 专业领域为机械或材料储运设备
  - 标准化对象为带式输送机
- 标准的类别为安全标准
- 标准的类型为规范标准

  可称为：国家机械产品安全规范标准

2 标准-强制性

标准

强制性标准

旨在保障健康和安全、保护环境，
为活动或其结果提供规程或规范，
由政府主导制定的强制实施的标准。

目的

功能

形成

目的维度：

- ✓ **国家安全**
- ✓ **人身安全和健康**
- ✓ **动植物生命和健康**
- ✓ **保护环境**
- ✓ **防止欺诈**

功能维度：

术语标准

符号标准

分类标准

方法标准

- ✓ **规范标准**
- ✓ **规程标准**

指南标准

规范（specification）：是规定产品、过程或服务应满足的技术要求的文件。适宜时，规范宜指明可以判定其要求是否得到满足的程序，便于验证。

规程（code of practice）：是为生命周期的有关阶段推荐良好惯例或程序的文件，用于直接进行操作。

3 标准化文件

10 其他标准化文件

- 通过标准化活动，不完全按照或没有按照标准制定程序制定，为各种活动或其结果提供规则、指南或特性，供共同使用和重复使用的文件

- 规范和规程——未完全履行标准制定程序
  - 技术规范 TS
    - **ISO/TS、IEC/TS、EN/TS**
  - 可公开获得规范 PAS
    - **ISO/PAS、IEC/PAS、BS/PAS、DIN/PAS**
  - 指导性技术文件
    - 国家标准化指导性技术文件 **GB/Z**
  - 企业规范或规程
    - 企业设计规范、企业工艺规程

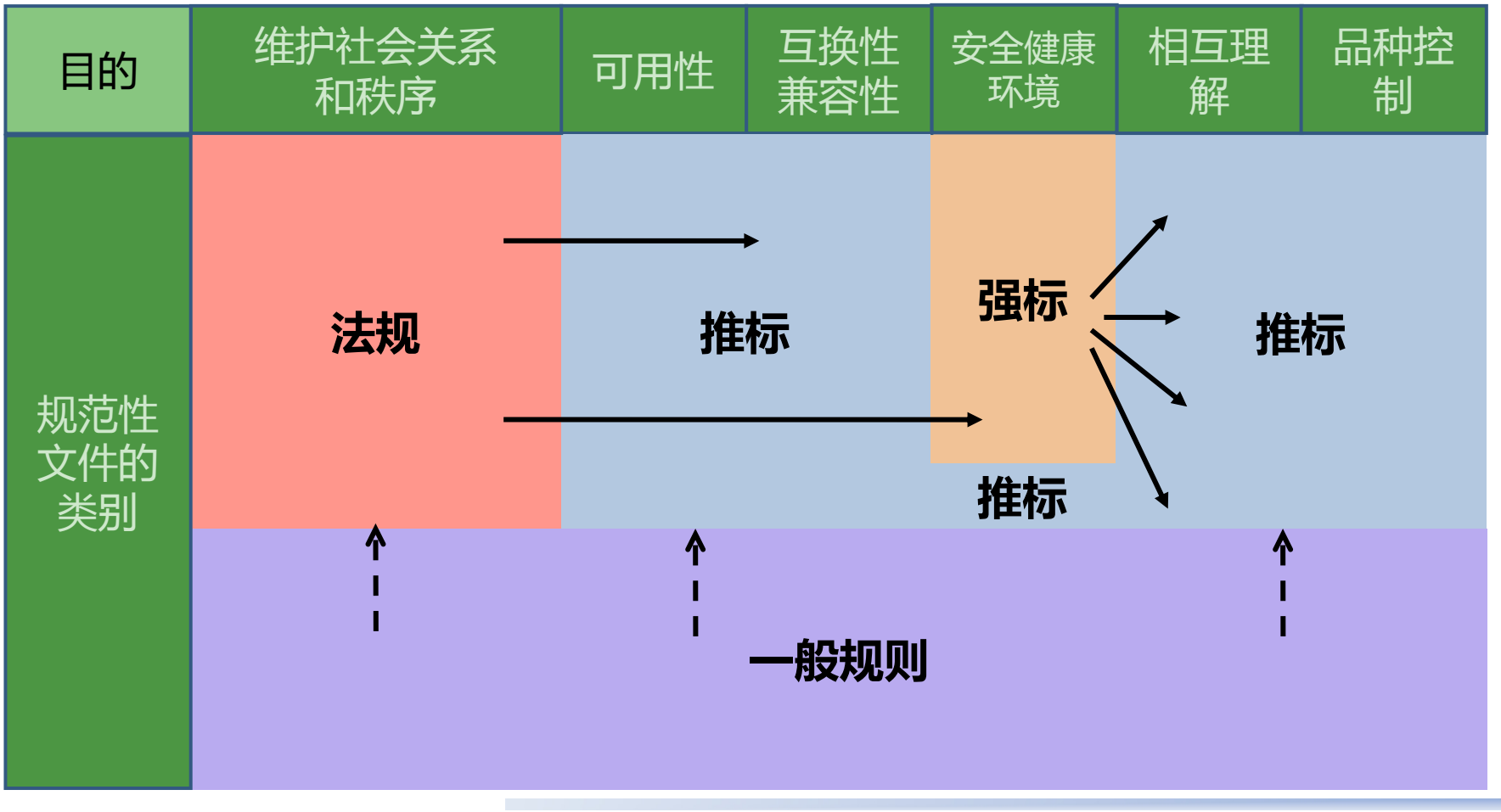
3 标准化文件

- 技术报告 TR——未完全履行标准制定程序，内容特殊
  - ISO/TR、IEC/TR，欧洲标准化委员会（CEN）技术报告（CR），欧洲电信标准协会（ETSI）技术报告（ETR），AFNOR文献资料（FD），JISC技术报告（TR）
- 指南 Guides——履行特殊程序
  - ISO/guide、IEC/guide、CEN/CENELEC发布的guide、ETSI发布的guide等
- 协议 Agreements——没有按照规定的标准制定程序，而履行某种联合形式的制定程序
  - ISO的IWA（International Workshop Agreement）、CEN和CENELEC发布的CWA，IEC发布的ITA（Industry Technical Agreement）

4 标准在规范性文件体系中的地位

法规	强标	推标	规则
社会准则 •制定目的：维护社会关系和社会秩序 •核心内容：规定当事人权利和义务 •规定能做什么、不能做什么 •具有普遍约束力 •引用标准	**技术准则** •目的：保障健康、安全、保护环境 •为活动或其结果提供可操作的程序（规程）、可检验的技术要求（规范） •规定怎么做、做的结果 •强制实施 •引用推荐性标准，被法律法规引用	**技术准则** •目的：可用性……其他目标 •为各种活动或其结果提供规则、指南或特性 •规定怎么做、做的结果 •推荐使用 •被法律法规、强制性标准引用	**一般规则** •由大家公认，供群体成员共同遵守的制度、条例或章程 •书面形式的成文条例；或约定俗成、流传下来的不成文规定 •可以成为法律法规、标准的基础

4 标准在规范性文件体系中的地位



5 标准化的作用及效益

- 建立秩序——从“无序”到“有序”
- 确立规则、应用规则
  - 确立规则——对人类的活动或活动结果，提供公认的技术规则
    - 界定：……术语、……符号
    - 确立：……体系、……系统，……一般原则
    - 规定：……要求、……方法；……尺寸、……特性
    - 提供：……指南、……建议、……信息

5 标准化的作用及效益

- 建立秩序——从“无序”到“有序”
- 确立规则、应用规则
  - 应用规则——通过改进产品、过程和服务的适用性，建立了技术秩序
    - 减少了多样性，保证了可用性，增强了互换性、兼容性、互操作性，便于产品防护（eg 流水线，AK47）
    - 保障了人类的健康和安全，保护了环境，促进了资源的合理利用
    - 增进了相互理解等等。
    - 保证了法规 / 技术法规的有效实施

5 标准化的作用及效益

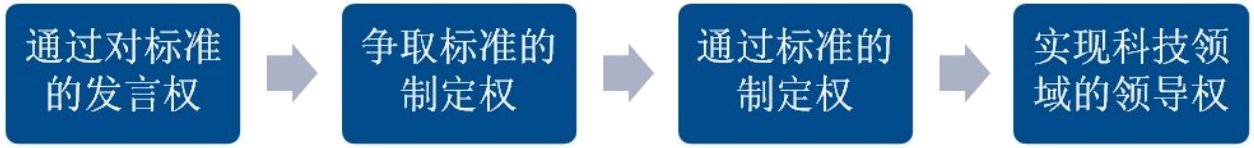
- 提高效率
- 保证产品和服务的质量
- 方便贸易交流，消除贸易壁垒
- 便利技术交流，提供创新平台

标准化作用与效益的产生源自有序化
（技术秩序的建立）

标准化的作用及重要性

标准化水平已成为各国各地区核心竞争力的基本要素：

性质	• 标准是规范市场经济客体的“法律”
地位	• 标准的战略地位日益突出
作用	• 标准是国民经济和社会发展的重要技术支撑
经济形势	• 标准是走向国际市场的“通行证”
发展趋势	• 标准是市场竞争的制高点



标准中的公权与私权

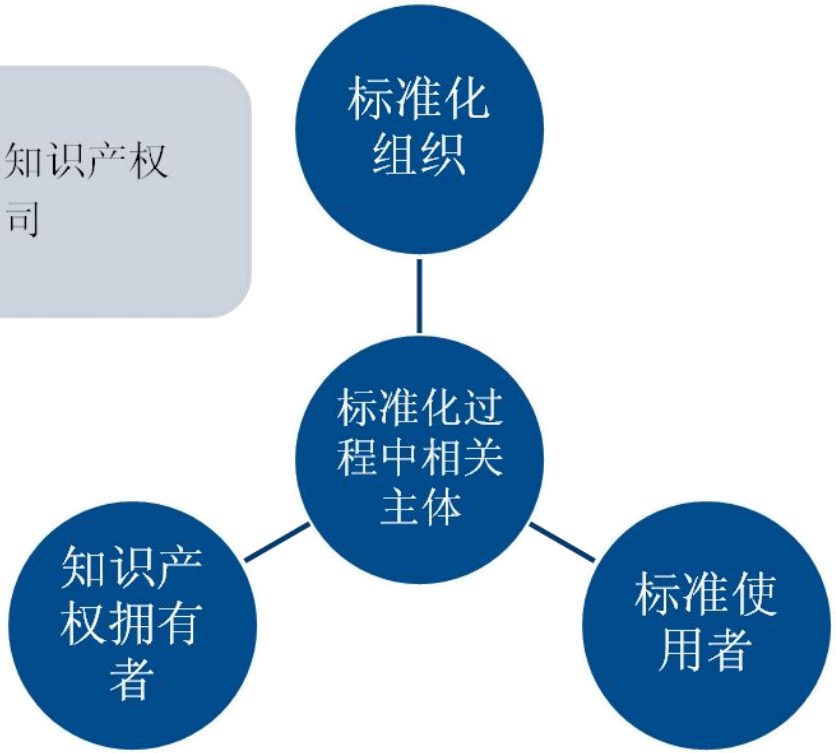
技术标准与知识产权之间存在着内在冲突

- 技术标准是公共产品或准公共产品，具有相当强的社会公共管理属性
- 知识产权是为激励创新而生的具有合法性、垄断性的私人财产权

形成市场壁垒（特别是技术标准为知识产权所覆盖）

- 赢家：掌控了技术标准中的知识产权
- 已经确立了事实标准的大公司

成果专利化 → 专利标准化 → 标准市场化



标准化的作用及重要性

拿破仑最引以为傲的不是他的赫赫战功，
而是他主导制定的《法国民法典》

秦始皇的伟大成就也不仅仅在于修筑了万里长城，而是统一了中国的度量衡

源远流长的标准化为人类文明的发展提供了重要的技术保障。

其 他

警惕领先国家的产品“污染”

范式威慑比产品污染更可怕

滥用标准与技术优势的影响

全球网络威胁

Reports show many zero-day exploits are auctioned / sold privately for future use

有报告表明，零日漏洞在暗地里拍卖，以备后用

Available data indicates a large majority of popular platforms is vulnerable to attack either directly or via add-on software

有数据证明，绝大多数平台可以被直接攻击，或被安装的软件攻击

It is clear existing exploits are used for fraud and data theft activities

很明显，现有的漏洞利用，被用于欺诈和盗窃

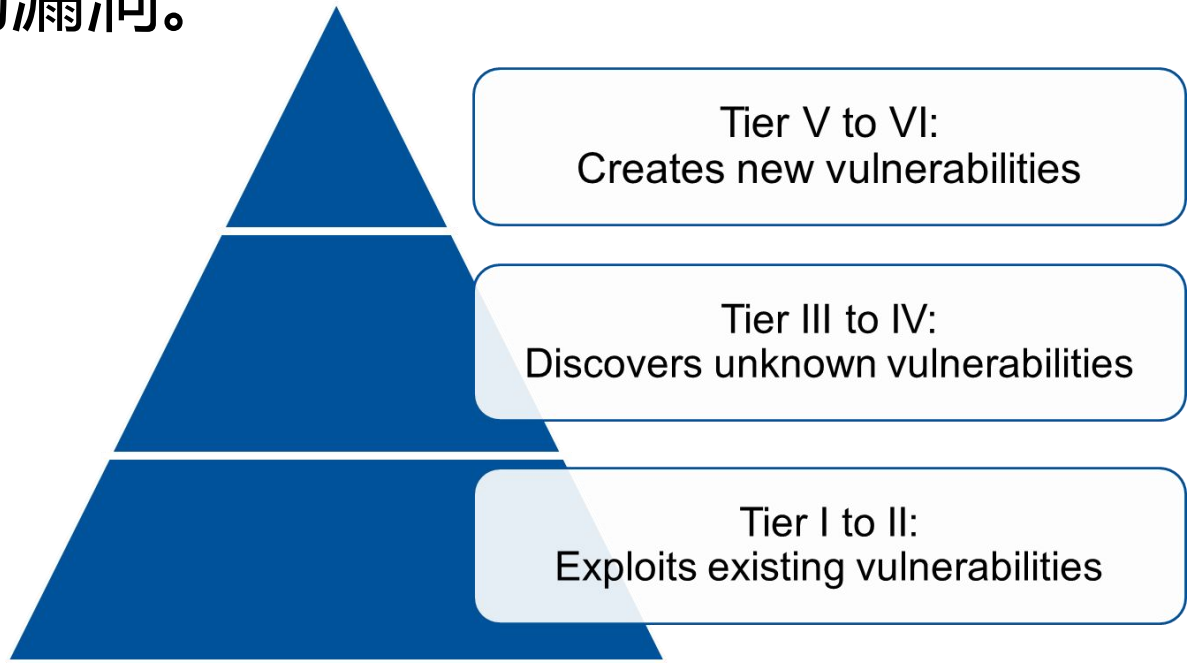
Is it less clear at this point whether the supply chain is being back-doored ？

但值得怀疑的是，供应链已经被安置后门了 ？

参考资料：Gartner

分层威胁模型

- 从分层的威胁模型来看，较低层次，是利用现有的漏洞；
- 中等水平层次，是发现漏洞；高级别层次，是制造出新的漏洞。



参考资料：Gartner

中国标准化：2013

国家标准：　　30374
备案行业标准：36481
备案地方标准：26980

国内　　TC：518；SC：704。
　　>ISO\IEC 900 TCs

问题：标准打架，缺失滞后，实施不力

TC260 信息安全标准化工作组

- WG1：信息安全标准体系与协调工作组
- WG2：涉密信息系统安全保密标准工作组
- WG3：密码技术工作组
- WG4：鉴别与授权工作组
- WG5: 信息安全评估工作组
- WG6: 通信安全标准工作组
- WG7：信息安全管理工作组
- WG8：

10位主任，8位秘书长

国际标准化组织–信息安全

ISO/IEC JTC1 SC27 信息安全标准化工作组

- WG1：信息安全管理体系
- WG2：密码学与安全机制
- WG3：安全评价准则
- WG4：安全控制与服务
- WG5：身份管理与隐私保护技术

标准组织工作布局

ITU-T SG17 安全、语言和通信软件

WP1-网络空间安全

Q1—安全项目组
Q2—安全架构组
Q3—安全管理
Q4—网络空间安全
Q5—反垃圾信息

WP2-应用安全

Q6—泛在网络安全
Q7—应用安全
Q8—云计算安全
Q9—生物信息安全

WP3-联盟身份管理

Q10—联盟身份管理
Q11—OID标准
Q12—安全基础设施(PKI)
Q13—软件语言标准
Q14—测试语言标准
Q15—开放互连标准

ITU-T SG13

- NGN、SDN、云计算、安全

ITU-T SG16

- 下一代网络的多媒体安全

标准组织工作布局

CCSA TC8 网络与信息安全工作委员会（工信部）

- WG1：有线网络安全工作组
- WG2：无线网络安全工作组
- WG3：安全管理工作组
- WG4：安全基础设施工作组
  云计算安全工作子组

公安部安标委

计算机信息系统安全保护等级标准；
应用系统安全等级评估检测标准；
计算机信息系统安全产品标准；
计算机信息系统安全管理标准等

标准组织关系

ITU-T、3GPP、IETF关系

- ITU-T和3GPP面向电信领域，

  强调需求—架构—组网

  协议层面尽量使用IETF的标准

- IETF面向互联网

  重点放在协议的制定--standard

  需求类标准—informational

  使用指南标准--informational

CCSA标准研究

CCSA标准研究

—移动互联网安全标准

— IPv6网络地址规划

- — 云计算安全
- — 网络身份管理
- —安全防护标准
- — 灾难备份
-

移动互联网安全标准体系

我国已经有一套标准体系，但这些标准

仍然不能有效指导解决现有的网络空间安全问题。

标准不是万能的，没有标准是万万不能的。

让我们共同努力，推进我国的信息安全标准化工作！

请大家批评指正！

谢 谢！