



the change challenges today's security thinking

# 安全国际化的挑战与机会

RSAC 2015@Beijing 挑战·机会·共赢

[alan.qian@huawei.com](mailto:alan.qian@huawei.com)

# Agenda

- 国际化的理由
- 国际化挑战
  - 信任关 市场准入关 知识产权关 安全关
- 国际化机会
  - ICT投资机会
  - 北斗的“复仇”
  - 国产化自主化与国际化
  - 专利与标准的格局
- 安全发展趋势预测

# 国际化的理由：拥抱全球化3.0



地球是圆的



世界是平的



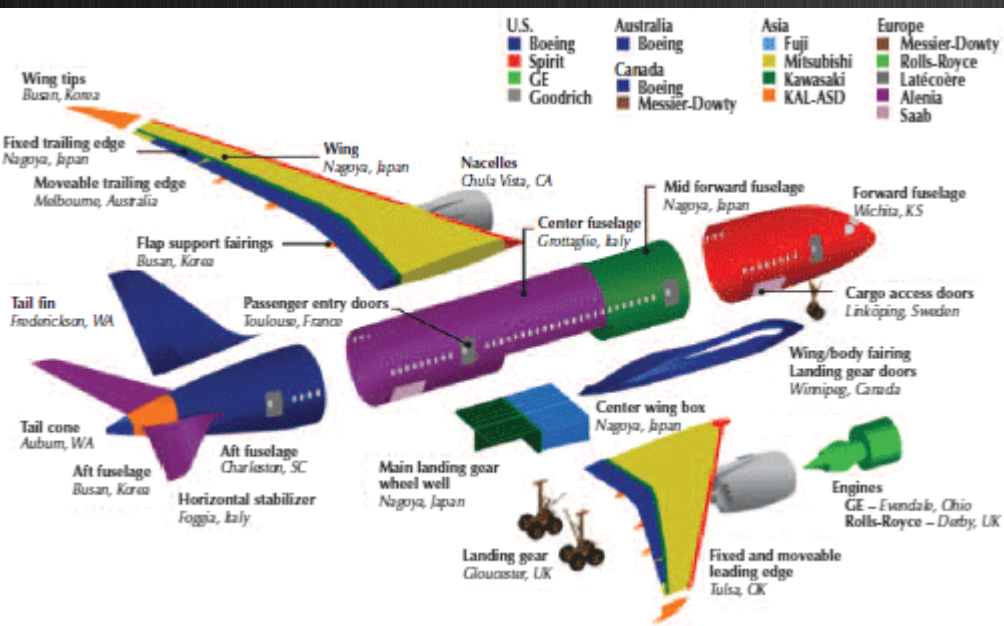
网络是全连接的



思维是互联网+的



# 国际化的理由：融入全球化供应链系统



您的手机，包含的器件可能来自世界各地——加拿大、爱尔兰、波兰、意大利、捷克、斯洛伐克一直到中国、以色列、日本、马来西亚、菲律宾、新加坡、韩国、台湾、泰国、越南和其他很多国家和地区。

中国成都，注册有16,000家公司，其中820家是外商投资公司。在这些公司中，189家为《财富》500强企业。一些家喻户晓的品牌也落户这里，举几个例子：Intel、微软、思爱普、思科、甲骨文、BAE、爱立信、诺基亚、波音、IBM和阿朗等。

思科公司，在中国6大城市设有研发中心，所有产品超过25%是由中国伙伴生产。思科曾在中国投资160亿美元，培训10万名网络工程师，并在职业技术学院成立300个中心给学生培训网络技术。这构成“国外开发”吗？

你中有我，我中有你



# 国际化的理由：改善安全产业格局

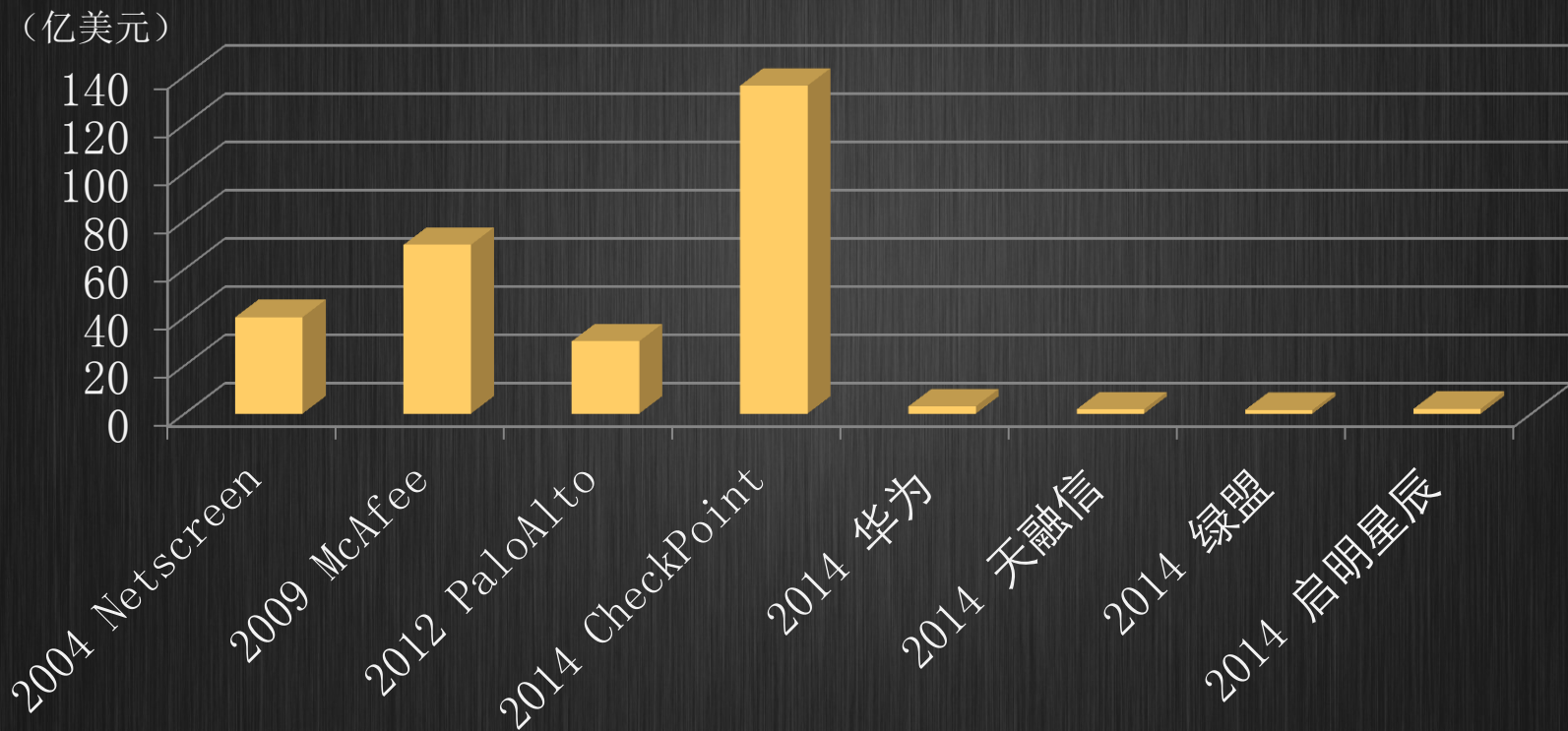


VS



1. 创业文化和专利保护。
2. 密切的产学研合作。
3. 完善的金融资本服务。
4. 丰富充足的中介服务资源。
5. 政府的宽松扶持政策。

# 国际化的理由：缩小安全企业的差距





# 国际化的理由：走快速发展之路

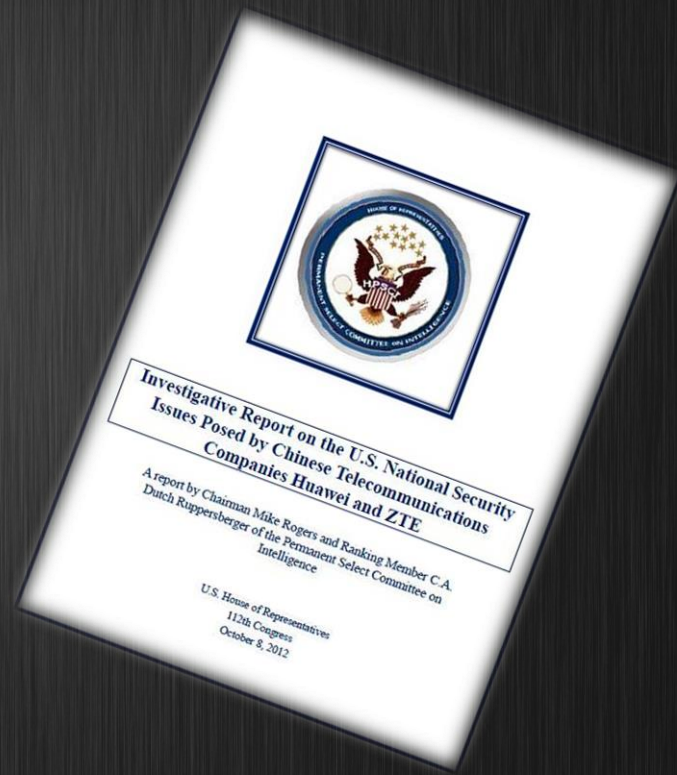


# Agenda

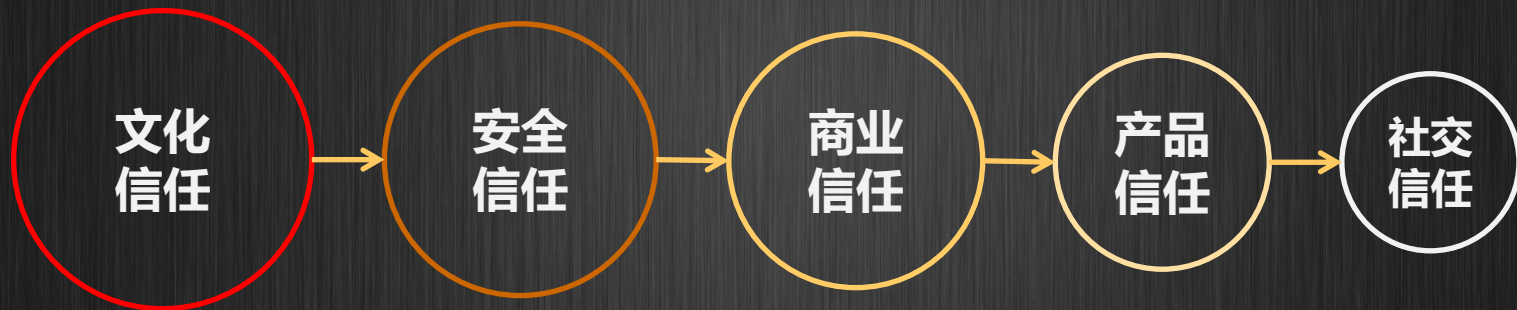
- 国际化的理由
- 国际化挑战
  - 信任关 市场准入关 知识产权关 安全关
- 国际化机会
  - ICT投资机会
  - 北斗的“复仇”
  - 国产化自主化与国际化
  - 专利与标准的格局
- 安全发展趋势预测











# 国际化挑战：信任关












# 国际化挑战：信任关



# 国际化挑战：准入关

区域	国家名称	认证类型	是否强制	认证标志图例
欧洲	欧盟	CE	是	
	瑞士	S+	是	/
	德国	TUV-GS	否	
	欧盟	WEEE	是	
独联体国家	俄罗斯	GOST R	是	
北美	美国	FCC	是	
		UL	否	
		FDA	是	
	加拿大	CSA	是	
		ICES-003	是	文字说明

区域	国家名称	认证类型	是否强制	认证标志图例
拉美	墨西哥	NOM	是	
	阿根廷	S-Mark	是	
澳洲	澳大利亚	A-Tick	是	
	澳大利亚/新西兰	C-Tick	是	
亚太区	韩国	MIC	是	 TE-A81K900-04-0309
	日本	VCCI	否	 <small>この機器は、クラスA電磁波障害物です。この機器を家庭環境で使用すると電磁波障害を発生させる可能性があります。この機器は、このマークを付した機器と近接して使用すると電磁波障害を発生させる可能性があります。 VCCI</small>
		DENAN	是	
		JATE	是	
		TELEC	是	
	新加坡	S-Mark	是	 1 2 3 4 5 6 - 0 0

## 强制认证违规后果

- 海关扣押
- 罚款
- 起诉
- 问题解决前禁止销售
- 强制货物回收
- 没收存货
- 市场禁入
- 监禁



# 国际化挑战：知识产权关

## ● 标准与专利的关系

标准的公开是为了推广技术，专利的公开是为了垄断技术

标准公开后没有任何保护，任何人可以免费使用；专利公开后强制垄断，未经许可任何人不得使用

专利需要利用标准来推广，同时标准需要专利的垄断来维护标准提案人的利益自主可控

## ● 游戏规则

专利所有者通过国际标准化组织将自己的专利变为标准，从而达到“挟天子以令诸侯”的目的

国际标准组织成为有权利和实力制定行业标准的国际巨头及标准推广的机器

而专利谈判，标准许可则是由垄断企业构成的标准联盟（行标，企标）决定。在这种谈判中，标准联盟往往处于谈判强力的位置，从而导致规则向标准联盟倾斜

在现有的游戏规则中，标准是各大厂商利益博弈的第一战场，所有国际巨头都在标准活动中投入重兵，以保证其在整个产业中的利益。专利成为了各大厂商在标准战场上进行搏斗的最直接的武器，这个武器的数量和质量直接决定了搏斗的解决。

# 国际化挑战：知识产权关

分类	主要玩家	活动表现	对企业的不利影响	对策	国内厂商可参与度
•专利壁垒	安全厂商和专利企业	海外专利诉讼	败诉会禁止销售或经济赔偿	积极申请专利以自保	强
•标准规范	安全与IT厂商/各国主管单位	•影响技术趋势，形成行业准则； •构筑产品准入门槛	•必须遵从优势企业制定的规则； •面临准入壁垒，增加产品成本	•遵从主流技术，并引导标准发展； •遵从公开的测评规范，积极参加测评认证	较强
•相关法律法规	各国政府，及所代表的利益集团	法律禁令	禁止进入市场	遵从目标市场法规	弱

# 国际化挑战：知识产权关

## 我国行业整体情况（中国国家知识产权局数据）

- 在信息安全行业，专利纠纷大部分发生在美国....
- 检索显示，美国、中国是全球信息安全专利技术最密集的地区。
- 在信息安全领域，我国企业的总体专利保有量已经逼近美国企业（正主动利用知识产权规则实现自保）

## 国外企业的规模和布局（2008年）

- 赛门铁克：财政收入60亿美元，公开全球专利约598篇、美国授权专利约326篇，待授权50篇。
- McAfee：收入约13亿美元，对应的专利数据分别是287篇、161篇和23篇。
- 趋势科技：收入接近10亿美元，对应的专利数据分别是88篇、28篇以及24篇。

## 2008年以来主要专利诉讼情况

诉讼发生地	涉及企业	涉及国家和地区
美国	趋势科技、赛门铁克、McAfee、微软、卡巴斯基等全球Top10 AV企业；阿拉丁、飞天技术公司等	美国、中国、日本

## 2015年安全专利诉讼情况

- 美国特拉华州地区法院2015年2月6日判决美国高智发明(Intellectual Ventures, IV)公司控告Symantec)的侵权胜诉。Symantec赔偿1700万美元。**IV还控告Intel、Check Point、McAfee及Trend, McAfee及Check Point已经分别和解。Symantec**发言人表示：由于裁定的赔偿数额远低于IV所要求的2.9亿美元的数额，因此对结果表示满意。IV获得了其所要求赔偿额的约6%。



# 国际化挑战：安全关（法规）

法律禁止的网络安全违法行为

非法监听/拦截

个人数据违法处理

个人数据违法转移

未授权访问

设备滥用

数据干扰

系统干扰

计算机犯罪

法律保护的权利

通信秘密及自由

个人数据及隐私

客户通信网络和信息安全

法律依据

欧盟：《网络犯罪公约》、《隐私与电子通信指令》、《欧盟数据保护指令》等

英国：《调查权限法》、《信息自由法》、《数据保护法》、《滥用计算机法》等

德国：《刑法》、《电信法》、《数据保护法》等

法国：《刑法》、《数据保护法》、《电子通信法》等

美国：《电子通信隐私法》、《计算机欺诈与滥用法》、《国家信息基础设施保护法》、《加强计算机安全法》等

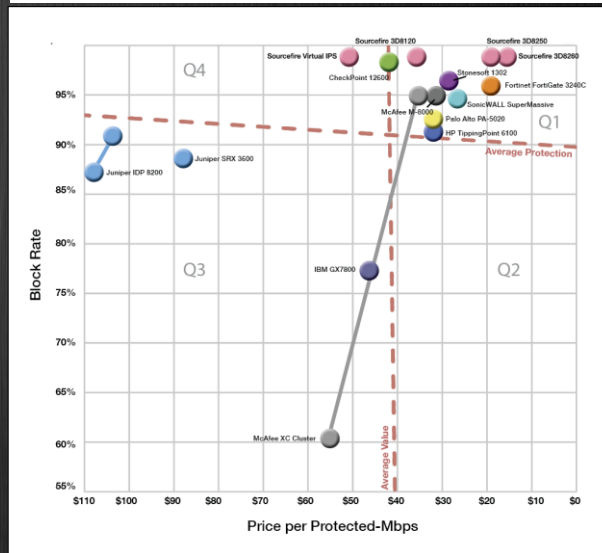
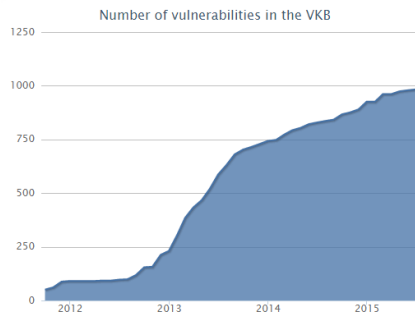
- 网络安全没有统一的法律法规，相关法律法规分散规定于国家安全、电信、刑法、数据保护等相关领域立法中，部分法律的违反可能直接导致行为人需承担刑事责任

# 国际化挑战：安全关（测试）



VKB specific to Telecom and Mobile networks

Overview Specifications Features Literature

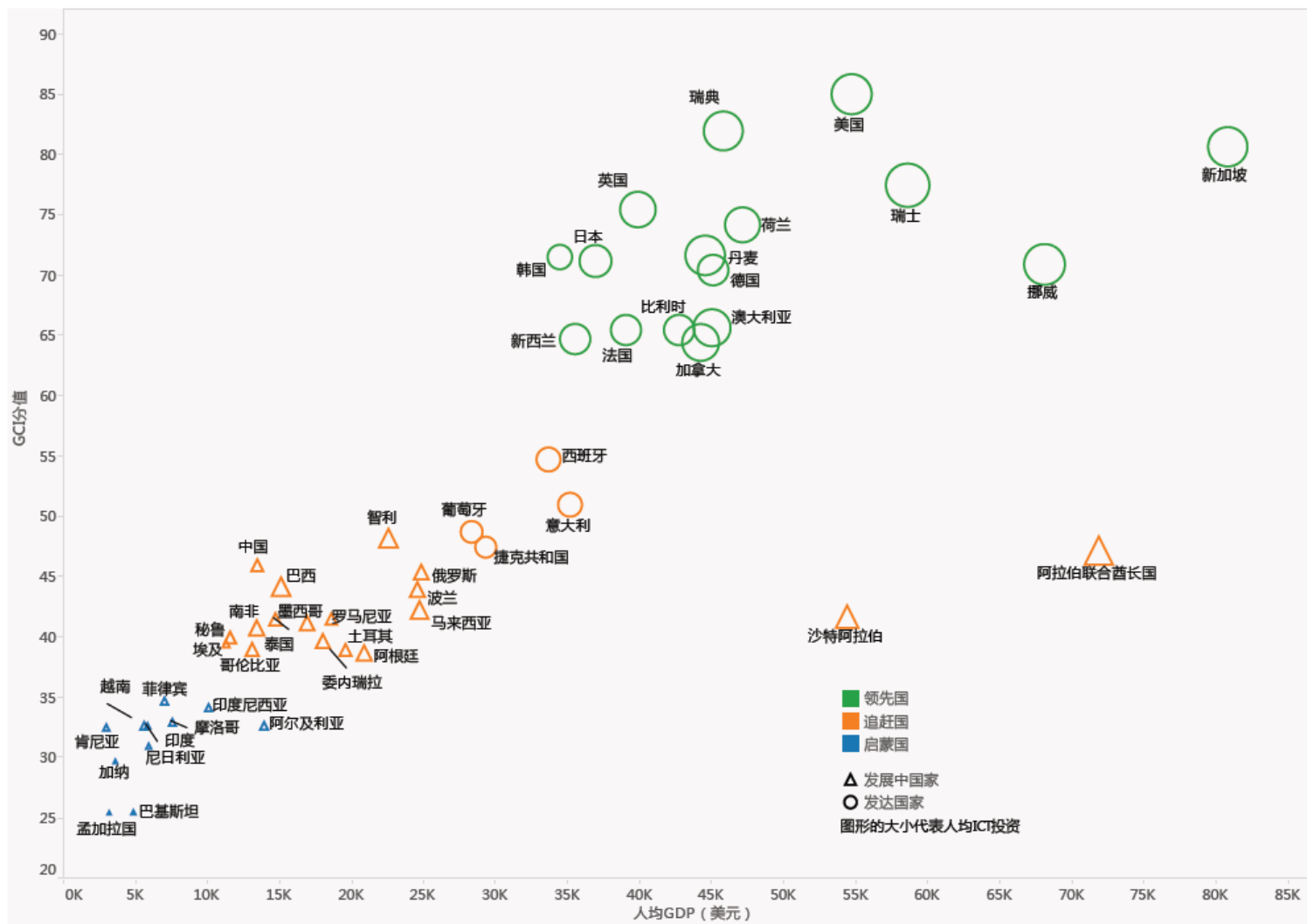


# Agenda

- 国际化的理由
- 国际化挑战
  - 信任关 市场准入关 知识产权关 安全关
- 国际化机会
  - ICT投资机会
  - 北斗的“复仇”
  - 国产化自主化与国际化
  - 专利与标准的格局
- 安全发展趋势预测



# 国际化机会：全球联接指数与GDP



# 国际化机会：全球ICT投资增长趋势



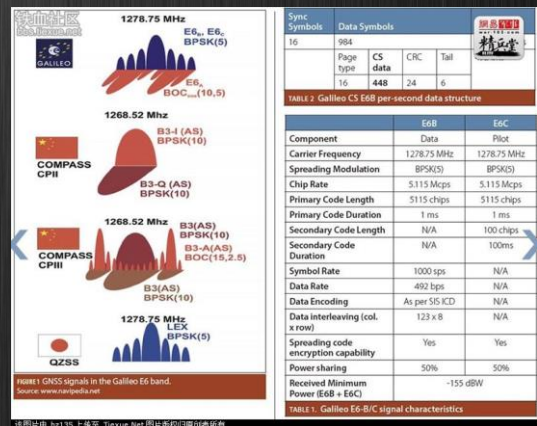
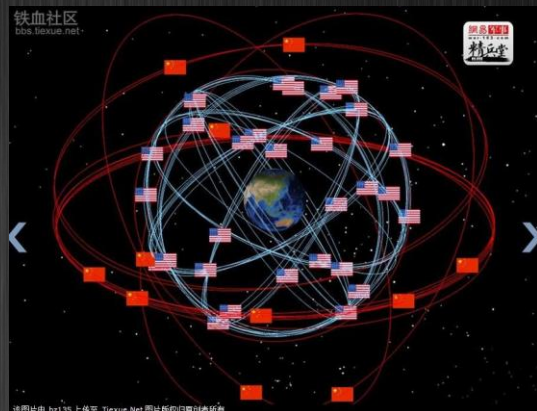
# 北斗的“复仇”

2003年，中国承诺投资2.7亿美元参加欧洲的“伽利略”全球导航卫星项目开发。但到2007年，中国突然被欧洲排除在所有“伽利略”项目之外，理由是安全和知识产权等问题。

2010年，中国领先欧洲发射大量北斗卫星，并基于PRS频段“先用先得”的规则，抢占了欧洲伽利略卫星的几个重要频段。欧洲可能觉得，将中国排除在伽利略计划核心圈，可确保自身的战略优势，美国也认为，ITAR有助于维持自己的战略优势。

2015年年初，中国卫星导航定位应用管理中心与欧盟代表团在捷克布拉格举行了北斗与伽利略卫星导航系统第四次频率磋商会谈。欧盟代表团接受了中国卫星导航定位应用管理中心提出的频率共用理念，同意在国际电联框架下完成卫星导航频率协调。中欧卫星导航系统结束了长达八年之久的频率协调工作，双方将携手合作走向共同发展。

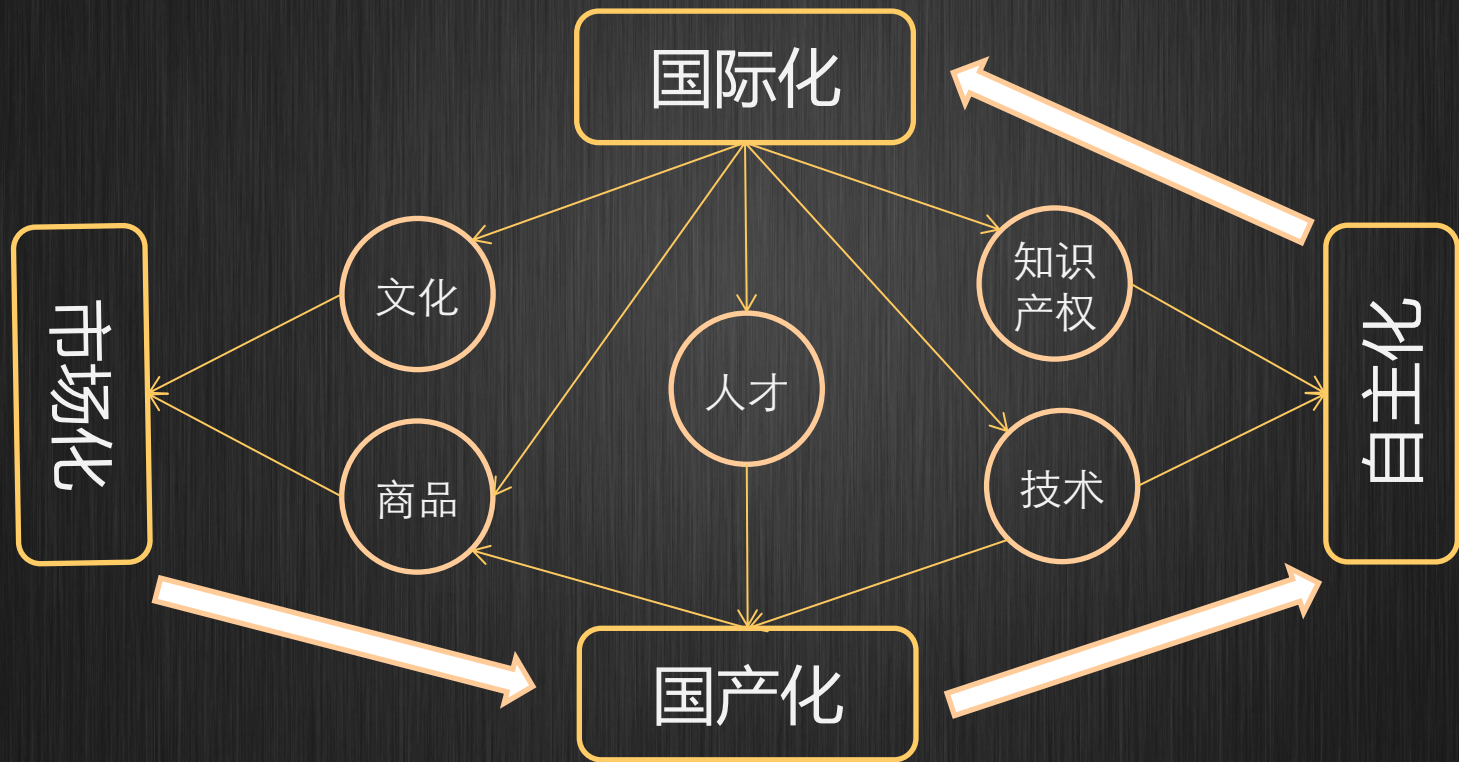
在战略行业排斥中国的做法，只会给其他全球参与者打开大门。最终损害的不是中国。若中国不能从欧美买到所需，它完全可以从零开始自主开发。



该图由 bu135 上传至 TieXue.Net 图片版权归作者所有



# 从国产化到国际化



# 积极拓展海外合作





# 解决安全难题

人机分别  
相似度判断  
相关性分析  
语义理解  
信誉评估  
大数据分析  
自动化提取特征或生成模型





# 国际化机会：安全技术标准格局

## 价值：

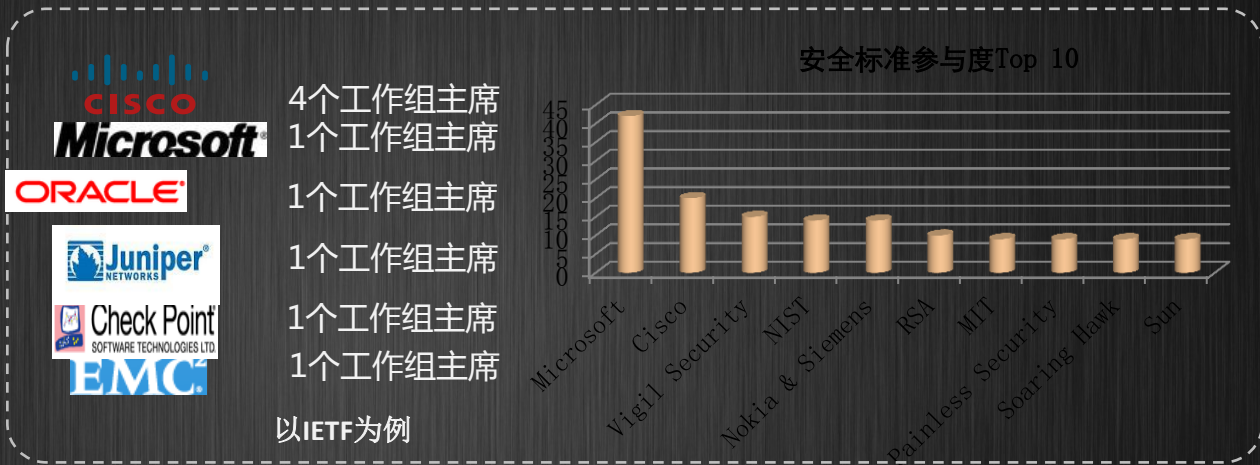
•安全标准无所不在，有利于形成公开规则，消除壁垒；

## 现状：

•安全标准被优势IT厂商所控制；  
•国外巨头，特别是美国，在国际标准制定中的影响力不容置疑；  
•国内厂商被迫处于不利地位；

## 对策：

•中国企业以追随为主，满足测评要求，通过努力影响标准制定，改变游戏规则。



工商  
商联  
联盟  
标准  
组织

各领先安全厂商均有代表参加标准活动



# 赢得国际化发展机会

1. 近年来全球网络攻击事件频发，引发市场关注。在各国政府推动下，网络安全的关注度日益提升，网络安全的重要性逐渐被认可，市场对相关解决方案的需求也不断上升，机构和企业相关开支有望大幅增长，相关市场或成为“蓝海市场”。当前正是投资网络安全行业的好时机，一些引领行业新发展方向的优势企业尤为值得关注。
2. 各国政府和企业对网络安全认识度的提升和重视，将推动防火墙、防范恶意软件、内容过滤以及加密工具等相关开支的增长。国际信息系统审计协会1月发布的**2015**年全球网络安全状况报告显示，在受访的**3400**个成员机构中，**83%**表示网络袭击是其面临的**最大威胁之一**，**86%**认为自身存在网络安全技术缺口，**92%**计划招聘更多网络安全专业人士。去年，摩根大通将网络安全开支提高到约**25**亿美元，并宣布配备**1000**名专业员工。美银美林CEO莫伊尼汉表示，网络安全是该公司**唯一没有预算限制的领域**。深圳市广道高新技术有限公司销售总监刘海军谈及，**2015**年我国网络安全产业规模将达到约**700**亿元水平，网络安全产业市场潜力巨大。
3. 市场研究机构**Markets and Markets**预计，未来几年全球网络安全预算将迅速增长，到**2017**年将达到**1200**亿美元，**2011**年至**2017**年的年复合增长率为**11.3%**。**FBR**资本市场分析师里夫斯预计，今年网络安全开支将增长**18%**到**20%**，相比之下整个IT板块的增速为**3%-5%**。**Gartner**数据显示，随着企业进一步扩大安全领域的技术投资，全球安全技术和**服务市场到2016**年将增至**860**亿美元。
4. 美国策略财富合伙人公司创始人兼总裁泰珀认为，网络安全是**2015**年最大的投资主题之一。至少在过去十年里，企业普遍在新技术方面投资不足，现在到了该领域开支加速的时候。网络安全行业将是企业技术开支增加的最大受益者。随着市场对网络安全解决方案的需求上升，以及网络安全行业日趋成熟，分析师认为现在正是投资相关企业的好时机，提供防病毒解决方案、数据备份和恢复、云系统、数据加密等服务的公司将因此受益。

# Agenda

- 国际化的理由

全球化3.0的机会

中美安全产业格局

- 国际化挑战

信任关 市场准入关 知识产权 安全关

- 国际化机会

自主可控 VS 国产化 VS 国际化 全球化的合作与协作 北斗经验

技术合作生态图景

- 安全发展趋势预测



# 安全发展趋势预测

- 1、随着沙箱与大数据分析产品的兴起，主要的技术挑战来自于更有针对性的高级对抗技术，包括anti-debugging、anti-vm、代码流混淆与数据污染等。
- 2、DDoS攻击与僵尸网络的治理进一步掀起“安全即服务”的云化运营高潮，并在运营商与数据中心以及安全厂商间形成商业模式。
- 3、新的威胁继续大面积爆发在互联网基础设施与主流基础软件上，如同2014的 OpenSSL Heartbleed以及 Linux bash 漏洞。
- 4、数字空间犯罪组织可能会针对互联网金融以及日益开放物联网与工控网发起致命攻击。
- 5、移动智能终端的安全直接影响人们的工作与生活，甚至影响到运营商的LTE网络。
- 6、国内出现开放的威胁情报共享组织，并快速形成行业联盟，推动更多安全厂商的产品基于标准实现设备与设备之间威胁情报交换，在线系统更加智能、敏捷，从而实现全网安全防御系统的实时协同。
- 7、企业与云数据中心更注重构建可持续的安全运维能力。更智能的安全运维平台、更高级的安全运维工具、更便捷的安全运维服务将广受关注。
- 8、中国网络安全法治化建设进入发展的快速通道，中国互联网安全治理形成政府与民间联手合作的双轨化运作。国内安全产业格局正在发生巨变，全球网络空间安全格局所受的深远影响也将逐步呈现。

互联网安全+

Thanks!