Development of ICT in Europe and Evolution of Information Security industry

ICT行业发展状况及信息安全产业的演变

Luigi Gambardella

www.chinaeu.eu

Content
内容

- Introduction of ICT industry in Europe
  欧洲ICT行业介绍
- ICT information Security in the 5G Environment
  5G环境下的ICT信息安全
- Current situation of Info Security in the EU
  欧盟信息安全现状

Source: European Commission, Europe's Digital Progress Report 2016
图表数据来源：2016欧洲数字进度报告，欧委会

Development of ICT in Europe
欧洲ICT行业的发展

Europe has the potential to lead in the global digital economy, but fragmentation and barriers that do not exist in the single market are holding back a healthy and uniform EU digital development. Bringing down these barriers could contribute an additional **EUR 415 billion** to European GDP, create opportunities for new start-ups and provide an environment for businesses to grow and benefit from **a market of over 500 million consumers**. This is precisely the goal of the **Digital Single Market Strategy for Europe**, adopted by the European Commission in May 2015.

欧洲有潜力领导全球数字经济，但单一市场不曾有的分裂和障碍却影响了欧盟数字经济健康、统一的发展。扫清这些障碍将为欧洲GDP增加4150亿欧元，同时为初创企业创造机会、并为企业的成长提供有利环境，而欧洲整体也将从这个有着5亿消费者的巨大市场中受益。而这也是欧盟数字单一市场战略的目标，欧委会于2015年5月采纳该战略。

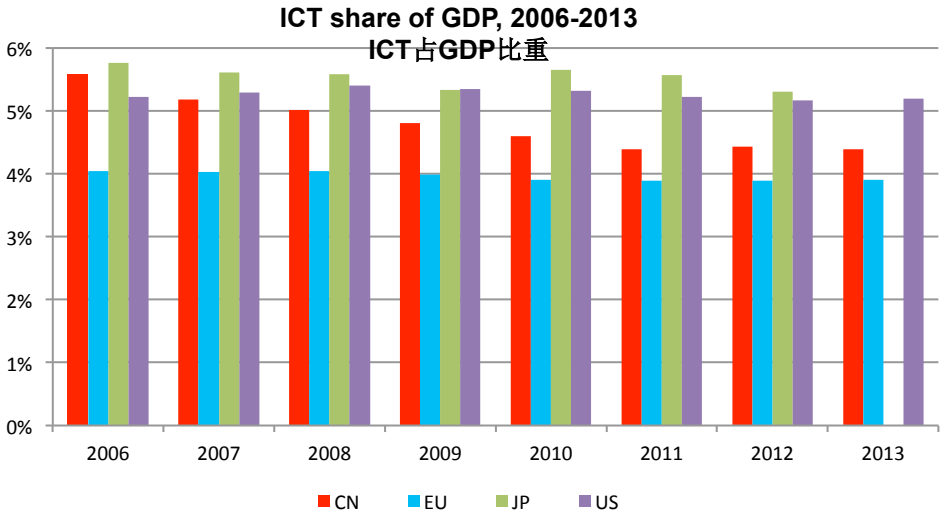
In April 2016, an initiative on **Digitising European Industry** was launched to link up national initiatives for digitising industry, such as *Industrie 4.0, Smart Industry* and *l'industrie du futur*, and mobilise up to **€50 billion of public and private investments** in support of the digitisation of industry.

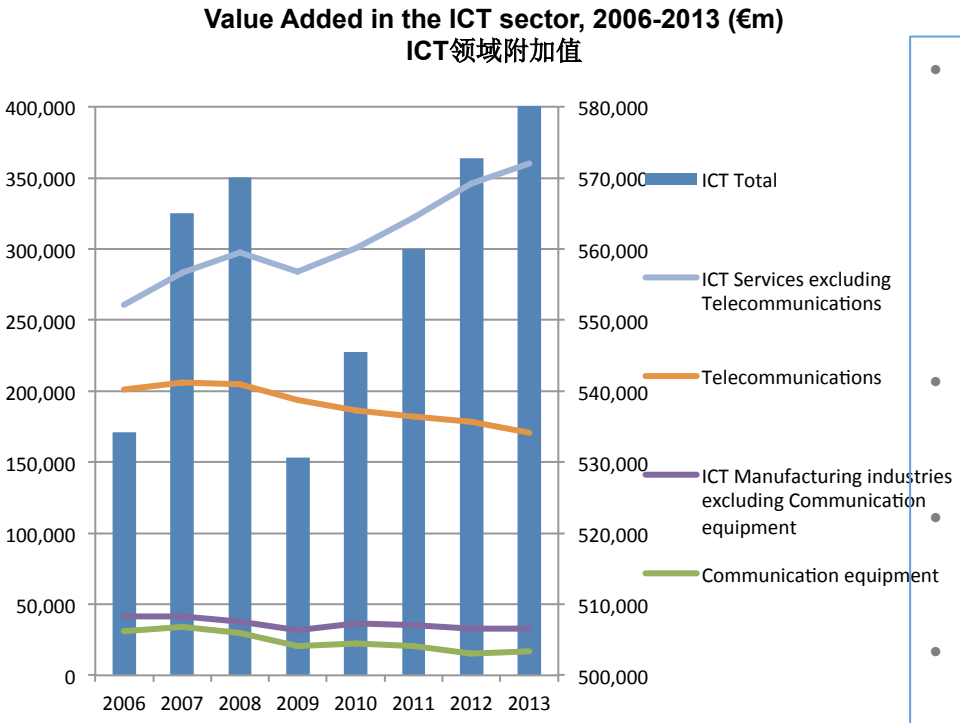
2016年4月，欧洲产业数字化倡议启动，连接所有国家层面的涉及产业数字化的指导方针，如工业4.0、智能工业、未来工业等。该倡议调动了500亿欧元的公私投资用以支持欧洲产业的数字化转型。

Value added in the ICT sector
ICT领域附加值

Value added in the EU ICT sector amounted to **€581 bn** in 2013, accounting for **3.9% of EU GDP**, behind China (4.4 %) and the US (5.2 %)

2013年欧盟ICT领域附加值达到5810亿欧元，占欧盟总GDP的3.9%，低于中国（4.4%）和美国（5.2%）





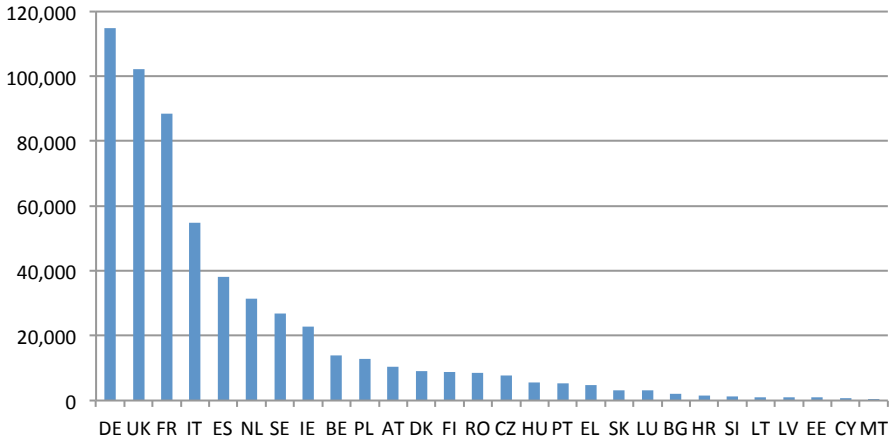
- **Predominance of ICT services** (€531bn and 91% of total ICT value added in 2013) over ICT manufacturing industries (€50bn and 9% of total ICT value added in 2013)
  ICT服务业（2013年附加值为5310亿欧元，占ICT总附加值的91%）相比ICT制造业（2013年附加值为50亿欧元，占ICT总附加值的9%）占主导地位
- **All subsectors declining apart from ICT services**
  除了ICT服务业外的其他部门都呈下滑趋势
- **Sharpest decline for the communication equipment** sector: after peaking at €34 bn in 2007, it fell to €17 bn in 2013, indicating structural decline
- 通讯设备部门下滑程度最严重：2007达到峰值340亿欧元之后，2013年滑落到170亿欧元，遭遇结构性衰退

ICT development across Member States
欧盟成员国ICT发展情况

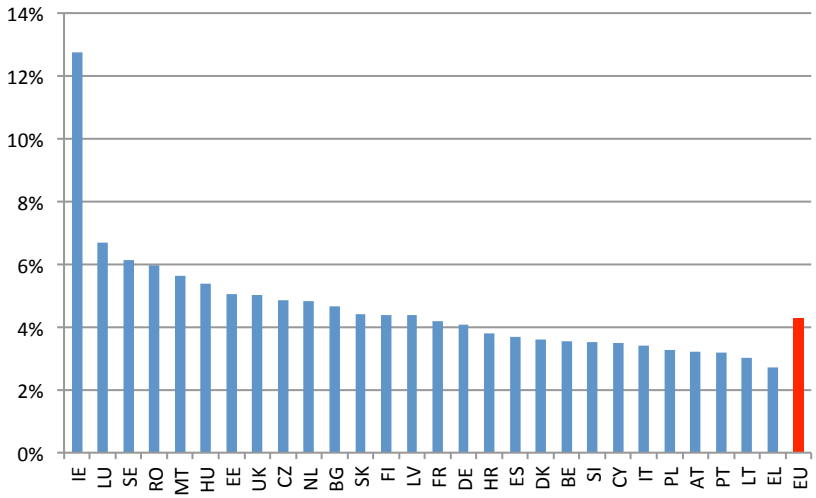
The **five largest economies** are also the five biggest contributors to ICT value added: **Germany** (€115bn or 20%), the **UK** (€102bn or 18%), **France** (€88bn or 15%), **Italy** (€55bn or 9%) and **Spain** (€38bn or 7%). Together, these five countries represented **69% of total** EU ICT value added in 2013.

前五大经济体同时也是对ICT附加值贡献最大的五个国家：德国（1150亿欧元/20%），英国（1020亿欧元/18%），法国（880亿欧元/15%），意大利（550亿欧元/9%）和西班牙（380亿欧元/7%）。2013年这五个国家ICT附加值加起来占整个欧盟ICT附加值的69%。

Value Added in the ICT sector, 2013 (€m)
ICT领域附加值



ICT share of GDP, 2013
ICT占GDP比重

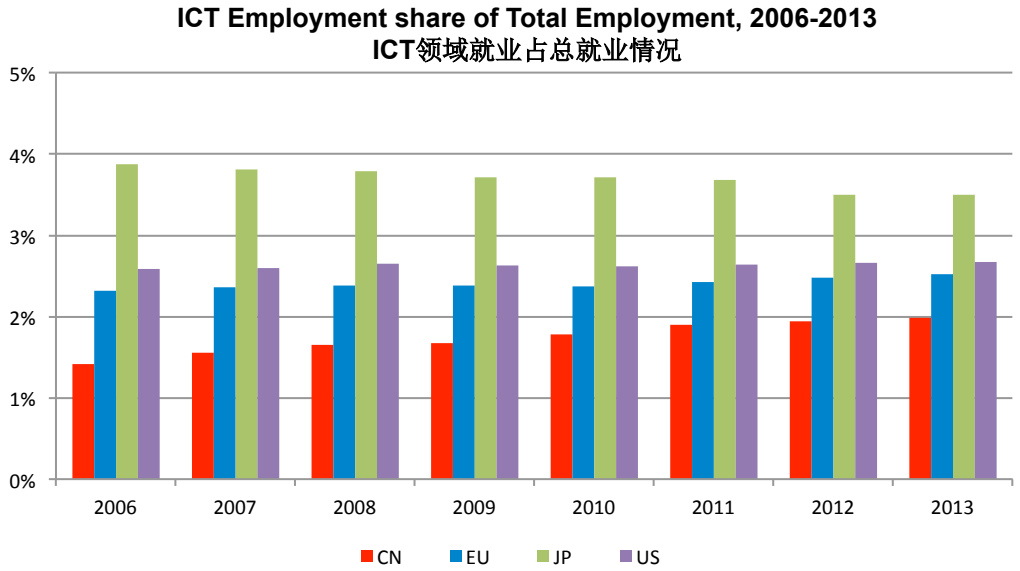


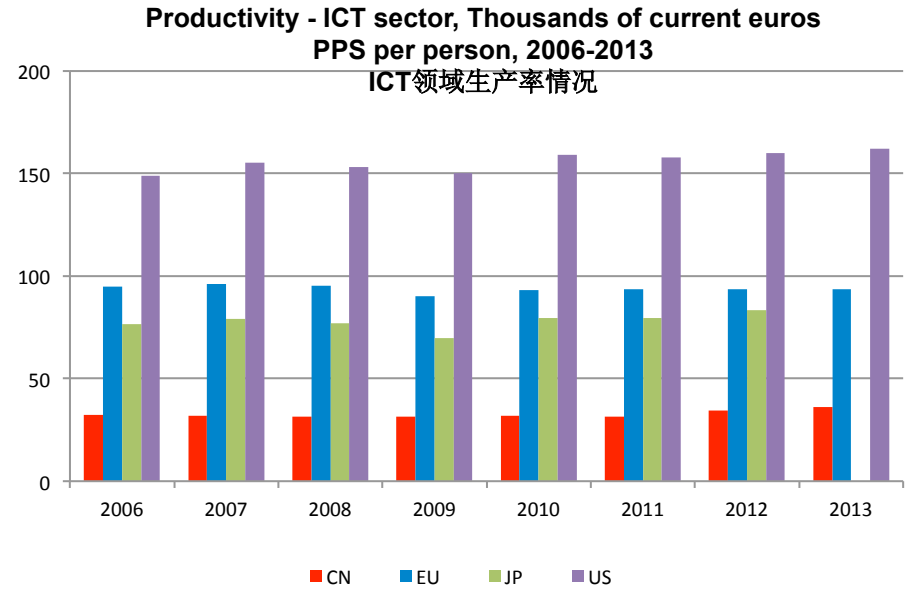
- **Ireland**: the highest ICT share of GDP (12.7%), followed by Luxembourg (6.7%) and Sweden (6.1%)
  爱尔兰：ICT占GDP比重最高（12.7%），其次是卢森堡（6.7%）和瑞典（6.1%）
- **Greece**: the laggard (less than 3.0%)
  希腊： 落后（少于3.0%）
- In most other Member States, ICT remained broadly stable as a proportion of GDP over period 2006-2013, except in Finland, where the rate fell by 4.2 pp
  在剩下的多数国家，ICT对GDP贡献在2006至2013年之间保持在一个稳定水平，但比率下降了4.2的芬兰除外

Employment and productivity in the ICT sector
ICT领域就业和生产率情况

The EU ICT sector employed **6.2 million** people, or **2.5% of EU total employment** in 2013, better than China (2.0%), but markedly behind Japan (3.5%)

2013年欧盟ICT领域就业者数量为620万，占欧盟就业总人数的2.5%，好于中国（2.0%）但仍明显落后于日本（3.5%）





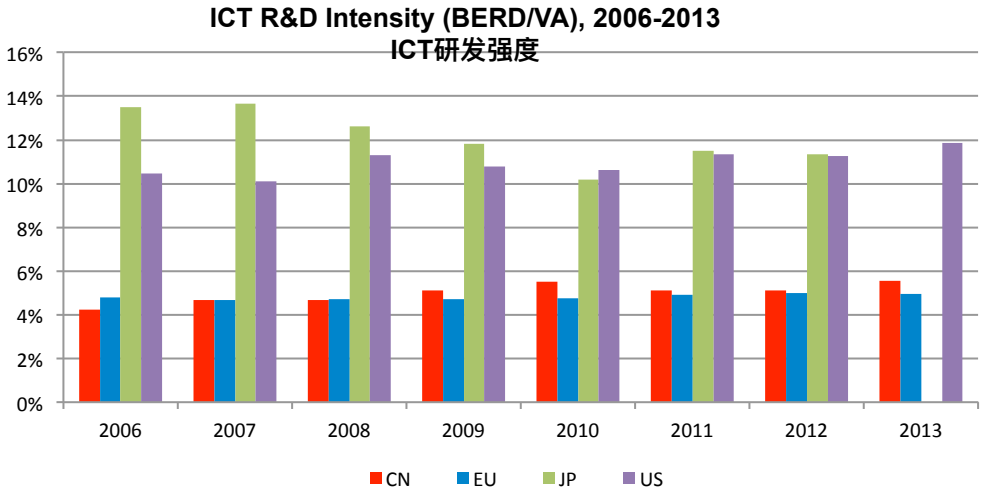
Regarding the **productivity** of the ICT sector, the EU (€93 000 per person) is behind the US (€162 000 per person), but far higher than China (€36 000 per person)

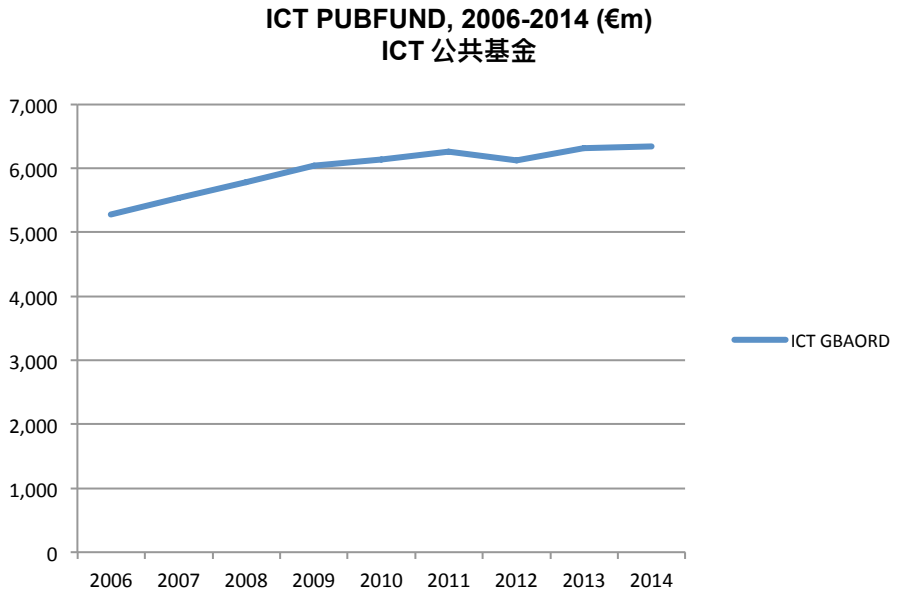
关于ICT领域生产率（93000欧元/每人），欧盟落后于美国（162000欧元/每人），但远远高于中国（36000/每人）

Private and public R&D expenditure in ICT
ICT行业公私研究与开发支出

Business enterprise R&D (BERD) expenditure in the EU ICT sector amounted to **€29bn** in 2013, or **5% of total R&D expenditure**, positioning behind China (5.5%) and far behind the US (11.8 %).

2013年欧盟ICT领域的商业企业研发支出达到290亿欧元，占研发总支出的5%，落后于中国（5.5%），与美国相距更加悬殊（11.8%）





The level of **publicly funded expenditure on ICT** R&D (ICT PUBFUND) in the EU reached **€6.3 bn**, representing **6.8 % of EU total government budget for R&D**.

欧盟用于ICT研发的公共资金支出达63亿欧元，占欧盟政府用于研发总预算的6.8%

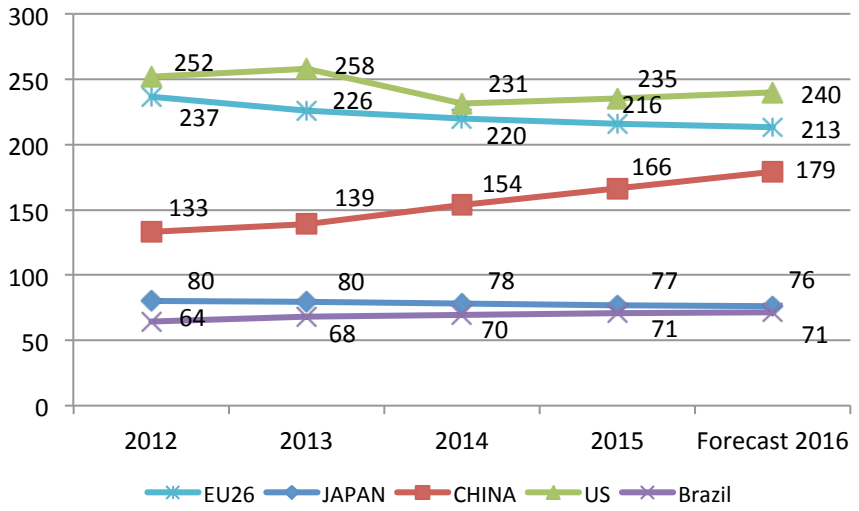
Telecom services revenues
电信服务收益

- **Total telecom services revenues have declined by 10%** in Europe since 2012, down from EUR 237bn in 2012 to EUR 213bn in 2016 (forecasted)
从2012年起欧洲电信服务总收益下降10%，（预计）2016年收益将从2012年的2370亿欧元跌至2130亿欧元

- Telecom operators in Europe generated less revenue than the US operators
欧洲的电信运营商相比美国电信运营商收益更低

- Large increases in emerging markets, especially in China
新兴市场的快速崛起，特别是中国

Total telecommunication services revenues per region, billion EUR, 2012-2016　　各区域电信服务总收益 （十亿欧元）

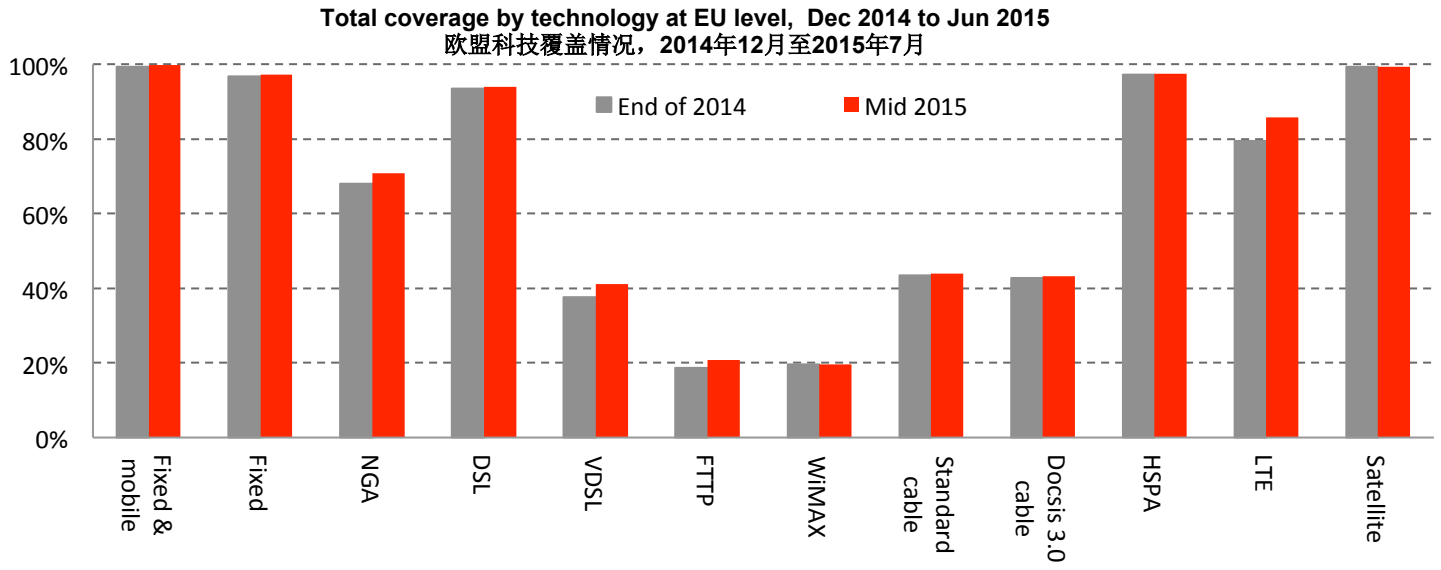


- **Mobile voice and fixed voice revenues have decreased by over 25%** since 2012
从2012年起移动声音和固定声音收益下滑超过25%

- **Mobile data grew by 10%**, and will represent over a quarter of total telecom revenues at EU level in 2016
移动数据增长10%，2016年这部分增长将占欧洲电信总收益的四分之一

Revenue growth rates 2012-2016 收益增长率	
Telecom carrier services 电信运营商服务	-10.0 %
Business data services 商业数据服务	-0.8 %
Fixed voice telephony 固定电话	-17.2 %
Internet access and services 网络接入和服务	13.1 %
Mobile data services 移动数据服务	9.9 %
Mobile voice telephony 移动电话	-30.8 %

Broadband coverage



Source: IHS and VVA

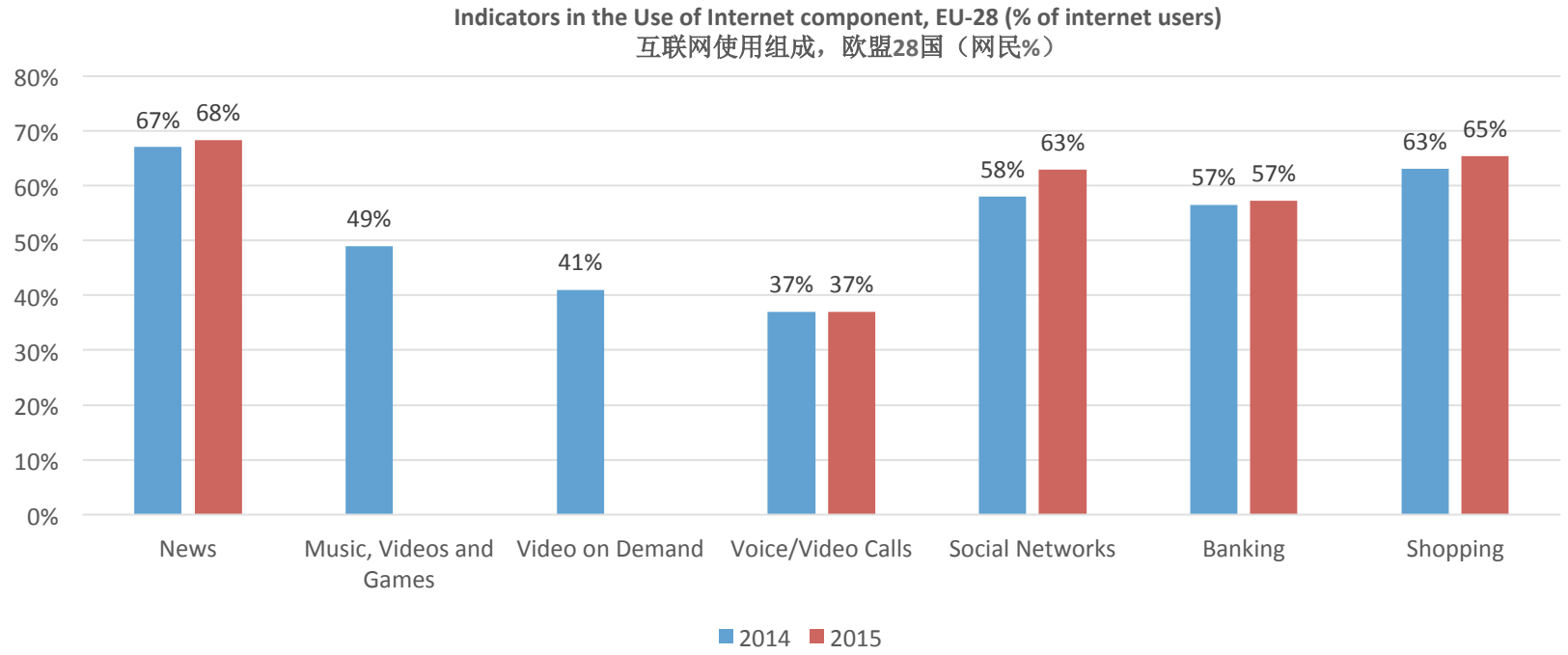
- Basic broadband is available to everyone in the EU
  欧盟境内所有人都可使用基本宽带
- Fixed technologies cover 97%
  固定技术覆盖达97%
- Next generation access (NGA) technologies (VDSL, Cable Docsis 3.0 and FTTP) capable of delivering at least 30 Mbps download are available to 71%
- 71%的人可以使用有能力达到至少30 Mbps下载速率的下一代接入(NGA) 技术（VDSL, Cable Docsis 3.0 和 FTTP）
- Deployment of 4G mobile (LTE) increased sharply and reached 86%
  4G移动技术发展(LTE) 急剧增长，覆盖率达到86%
- Rural coverage remains significantly lower, especially in NGA
  偏远地区覆盖率相比仍然很低，特别是对于NGA

EU Target 欧盟目标：

- **Basic broadband for all by 2013: 100% in 2015**
- **2013年所有人可使用基本宽带： 2015年覆盖率已达到100%**
- **Fast broadband (>30Mbps) for all by 2020: 71% in 2015**
- **2020年所有人可高速宽带(>30Mbps)：2015年覆盖率已达到71%**

Use of Internet in the EU
欧盟互联网使用情况

Internet users 网民数量	400 million 4亿
Penetration rate 渗透率	79%
Mobile Internet users 移动互联网使用者	218 million (55% of all Internet users) 2.18亿（展互联网使用者总量的55%）



ICT Information Security in the 5G Environment
5G环境下的ICT 信息安全

2000s: fixed broadband

2000s:固定宽带

2010s: 4G

2010：4G网络

2020s: 5G

2020：5G网络

Hardware: fibre and transmission equipment

硬件：光纤和传送装备

Higher ‘layers’ : Innovation

高“层”：创新

Service levels: applications that will be conveyed over the new networks

服务层：新网络所传送的应用

Opportunities and Challenges in IoT
物联网领域的机遇与挑战

- Combining IoT and big data technologies will enable new, big business opportunities
  互联网和大数据的结合引发了巨大的新商机
- A growth in IoT solutions market value from $1.9 trillion in 2013 to $7.1 trillion in 2020 (IDC Analysts)
  预计到2020年，物联网解决方案的市场价值将从2013年的1.9万亿美元增长到7.1万亿美元 （IDC Analysts）

- Data protection concerns could nevertheless constitute a major obstacle to larger scale rollouts of these activities.
  但关于数据保护的考量将成为这些新商业活动大规模展开的一个主要阻碍
- Connected machines will create huge network security, or better IoT security challenges
  而设备间的互联也将对网络安全，或者说对开发更好的物联网安全提出严峻挑战

- Security is a threat, but also an opportunity
  安全问题是威胁，但同时也意味着机遇
- only 32 % of enterprises in the EU had a formally defined ICT security policy
- 欧盟各成员国中只有32%的企业具有正式定义的ICT安全政策

The importance of Certification 认证的重要性

- Certification constitutes a growing market: Smart cars, machines, plants and buildings will all need to be reviewed and certified
  认证市场正在不断发展：智能汽车、设备、工厂和建筑都将需要被评估和认证
- Problem: Limit to the number of players--trust and reputation are by nature linked to strong brands
  问题：对参与者有局限0--信任和声誉自然而然地会倒向大品牌

Opportunities and Challenges in online gaming
在线游戏领域的机遇与挑战

The global gaming software market is expected to grow from 57.6 billion EUR in 2015 to 81.7 billion EUR in 2019.
全球游戏软件市场增长迅速，预计到2019年，该市场有望从2015年的576亿欧元增长至817亿欧元。

Example of security challenge:
安全挑战的案例：

online in-game currency steeling through reversing engineer the game's source code and thus creating a game simulator that sent fake completed match statuses to the servers of the on line game operator
骗取在线游戏币：通过改变一款游戏程序员的源代码从而创造一个给在线游戏运营商的服务器发送假信息的游戏虚拟器

The growth of on-line gaming thus also constitutes a new workplace for the development of security solutions.
在线游戏市场的不断成长也为网络安全解决方案的发展打开了一个全新领域

Opportunities and Challenges in eHealth
数字卫生领域的机遇与挑战

The medical IoT is set to transform healthcare through smart medical devices. However, their success is in jeopardy if cybersecurity concerns are not addressed simultaneously.
医疗物联网通过智能医疗设备转变传统健康服务模式，但若不能同时解决网络安全所带来的隐患，那么其成效将受威胁

$390 million of the $5.5 billion spending by healthcare providers and OEMs on healthcare cybersecurity, will be dedicated to securing medical devices (ABI Research): embedding security in the hardware, reviewing, analyzing, pen testing, developing patches, performing over the air updates, data protection…
医疗服务提供者和原始设备设备制造商在医疗网络安全的花费是550亿美元，其中只有3.9亿美元用于保障医疗设备（ABI Research ）：在设备硬件中嵌入安全装置、评估、分析、贯入试验、修补程序研发、线上更新执行、数据保护…

critical vulnerabilities of medical devices: code errors in software, use of hard coded passwords, disabling of firewalls, lack of authentication mechanisms, unencrypted communications…
医疗设备的几个核心弱点：软件编码错误,使用硬编码密码、使防火墙瘫痪、缺乏鉴定机制、非加密沟通等…

- collaboration across the various stakeholder silos is necessary to address technical issues, healthcare delivery, and business challenges needed for protecting devices
- 为解决保护设备安全所需的技术问题、医疗成果交付和商业挑战，社会各界之间的协同合作是必须的
- public authorities can (and should) set the basic requirements, it is up to the market players to come up with security solutions and certification of devises and processes
- 政府和当局可以（也应当）设立基本的规则框架，但是具体的安全解决方案以及设备和过程的证书还是取决于市场各参与方

Current situation of Info Security in the EU
欧盟信息安全现状

- Member States have very different levels of preparedness

  各成员国的准备水平参差不齐、相差悬殊
- Fragmented approaches across the EU

  欧盟境内未形成处理信息安全的一致系统途径，欧洲网络安全市场碎片化程度较高
- Unequal level of protection of consumers and businesses

  对消费者和企业的保护水平不等
- Lack of common requirements on operators of essential services and digital service providers

  缺乏针对核心服务运营商和数字服务提供商的一般性要求

The Network and Information Security (NIS) Directive
欧盟网络与信息系统安全指令

- EU Member States must transpose the Directive by 9 May 2018 into their national laws.

  欧盟各成员国需在2018年5月9日之前将本指令内容纳入各自的国家法律中

- Member States must oblige the following undertakings to report cybersecurity breaches:

  各成员国必须强制涉及下列领域的企业在发现或发生网络安全事故后及时向本国相关机构汇报
  - operators of essential services in critical sectors such as energy, transport, health and finance; and

    能源、交通、健康和财政等关键领域的核心服务运营商，以及
  - providers of 'digital services' – defined as online marketplaces, search engines and cloud computing services

    "数字服务"提供商–指在线市场、搜索引擎和云计算服务
- EU member states to raise cyber security capabilities

  欧盟各成员国须提升网络系统安全并加强防范风险和处理事故能力

- Two new EU coordination groups are set up:
- 新成立两个欧盟协调工作组
  - a Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among member states, and
  - 一个用以支持和协助各成员国之间战略合作及信息交流的协调小组
  - a network of national Computer Security Incident Response Teams (CSIRTs), to promote swift and effective operational cooperation on specific cybersecurity incidents
  - 一个国家级计算机安全事故响应小组(CSIRTs)的联络网，用以促进各国间针对网络安全事故开展及时有效的业务合作

- These two new groups will already start work in February 2017.

  这两个新的工作组将从2017年2月起正式开始工作

Key Area of Info Security in the EU
欧盟信息安全的关键领域

Follow-on to the NIS Directive 对欧盟网络与信息系统安全指令的进一步跟进

As a follow-on to the NIS Directive, the EU Commission 为近一步跟进NIS指导，欧委会:

- will present in the first half of 2017 to the Cooperation Group, the CSIRTs Network and "*other relevant stakeholders*" a blue print for how to respond in a coordinated way to a large scale cyber incident involving several member states.
  将于2017年上半年向根据指令建立的合作团体、CSIRTs网络和"其他相关机构"展示一份阐述如何协同应对涉及多个成员的大规模网络安全事故的蓝图
- will create an information hub to support the exchange of information between EU bodies and member states
  将创建一个信息中心用以支持欧盟机构和各成员国之间的信息交流
- launched a Public Private Partnership on cybersecurity launched in July 2016. Expected to trigger €1.8 billion of investment by 2020 to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector
  于2016年7月启动网络安全公私合作伙伴关系，并计划在2020年前投资18亿欧元，以期欧洲得以更好地应对网络攻击并加强其网络安全部门的竞争力

Member States must 各成员国须:

- adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cybersecurity
  制定本国的NIS战略，定义网络安全相关的战略目标、治理政策和管理规范
- designate one or more Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks
  建立至少一个CSIRTs负责国家层面的网络安全事故和风险

Key Area of Info Security in the EU
欧盟信息安全的关键领域

Further action in the pipeline 未来行动

ANNOUNCED BY EU COMMISSION
欧委会已宣布的

Certification 证书

- possible European certification and labelling framework for ICT security products
  可能会有针对ICT安全产品的专门证书和标签
  - roadmap by the end of 2016
    2016年底前发布白皮书
  - proposal by the end of 2017
    2017年底前提交提案

Institutional 机构的

- Reassessment European Union Agency for Network and Information Security – ENISA, whose mandate comes up for renewal in 2020
  重新评估欧盟网络与信息安全的机构–欧洲网络与信息安全局，其受命进行的工作将于2020年进行更新
  - roadmap published on July 25, 2016
    2016年7月25日发表白皮书
  - Evaluation to be completed by the end of 2017
    2017年底完成评估
- https://www.enisa.europa.eu/

THANK YOU!
谢谢！

www.chinaeu.eu
President@chinaeu.eu
Schuman 6/5, 1040 Brussels