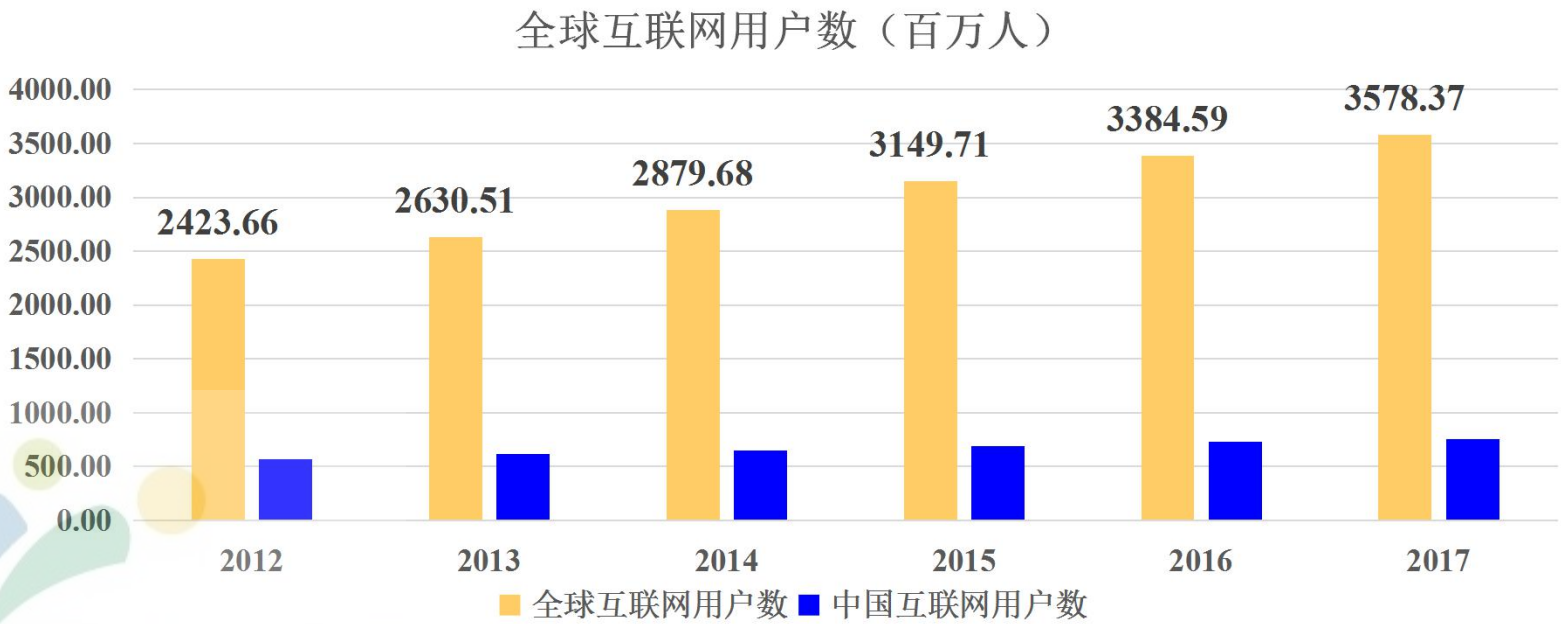
中国互联网安全状况探讨

中国（合肥）互联网大会

倪光南　合肥　2017.11.24

前言：2017年全球联网人数超过35亿

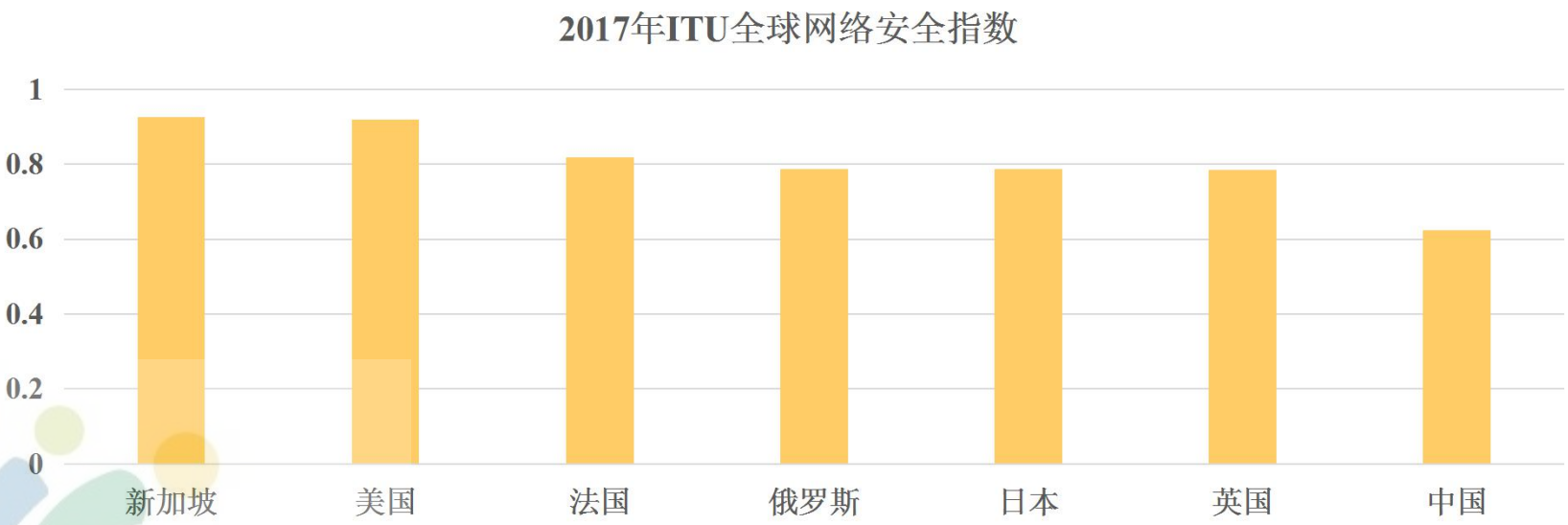


ITU预测，2017年全球联网人数达到35.78亿，占全球人口数的48%。其中，中国互联网用户数达到7.51亿，占全球21%。保障网络安全越来越成为一个全球性的重大问题。

物联网设备首次超越人口数

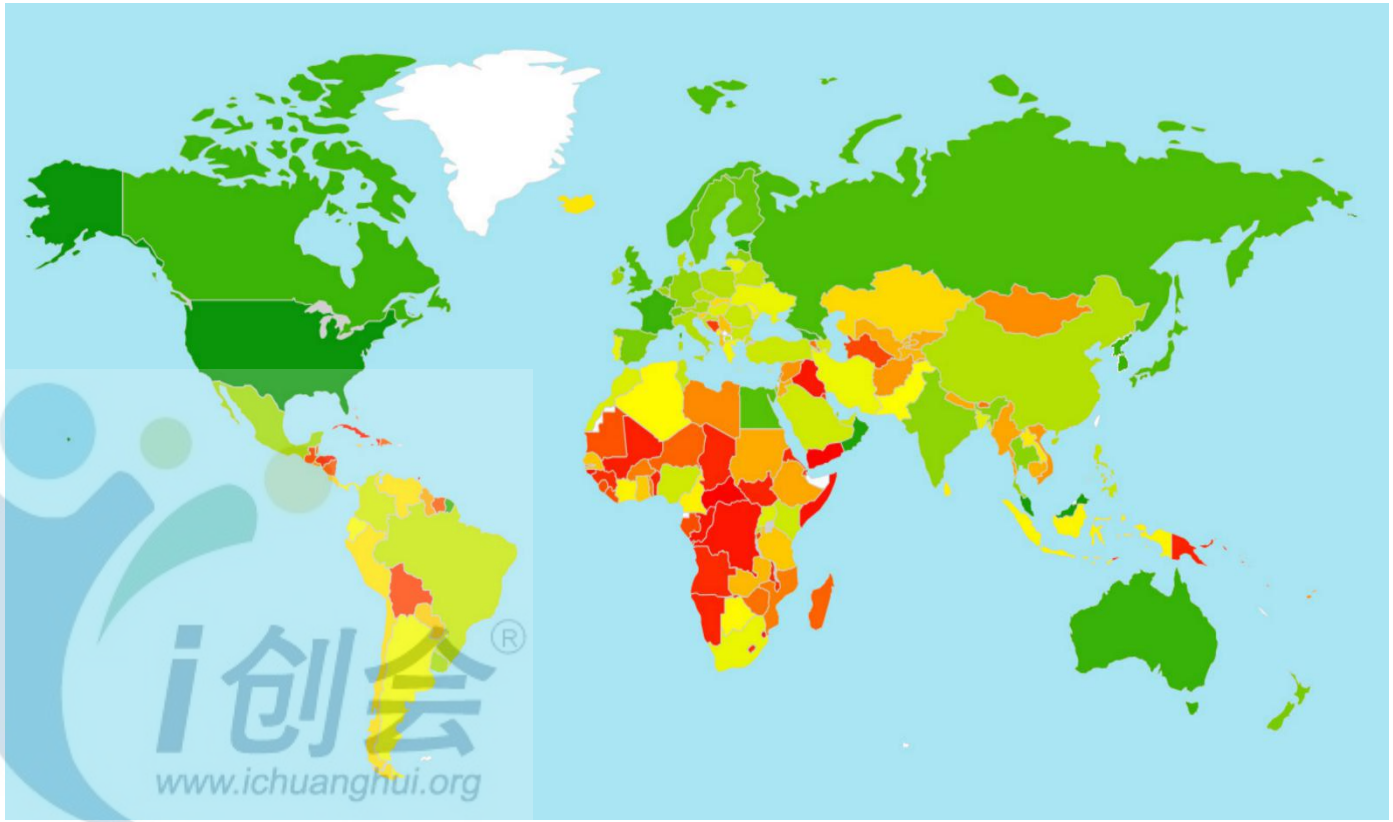
根据Gartner数据，2017年，全球联网设备数量达到84亿台，比2016年的64亿增长31%。2017年全球人口数量75亿，联网设备数量首次超越人口。物联网的安全问题也同样会造成严重威胁。

全球网络安全指数提升



2017年，ITU全球网络安全指数相对2016年有提升。ITU将193个国家的安全战略划分为三个阶段，有21个国家出于领先阶段。中国排名32，位于成熟阶段。

38%国家发布网络安全战略



目前，38%的国家发布了国家安全战略，另有12%的国家正在制定网络安全战略。不过仍有50%的国家毫无安全战略。

网络安全大事件

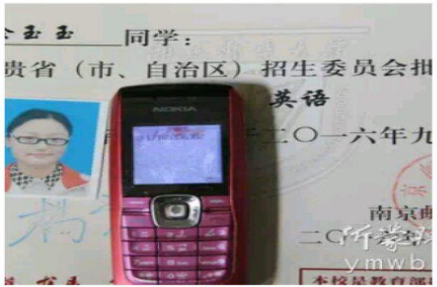
一、“徐玉玉”事件唤醒全民网络安全意识

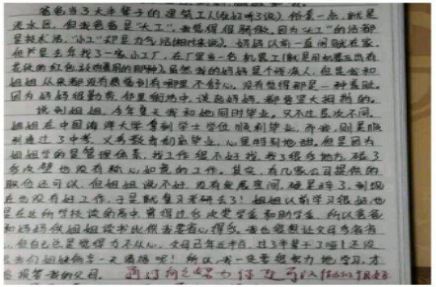
二、“Mirai病毒”宣告僵尸物联网的到来

三、“永恒之蓝”勒索病毒全球爆发

一、“徐玉玉”事件唤醒全民网络安全意识

【18岁女孩被骗学费9900元 郁结于心离世💔】今年高考，临沂女孩徐玉玉被@南京邮电大学 录取。19日她接到陌生电话，称有笔助学金要发放给她。因之前接到过教育部门的通知，徐玉玉便没有怀疑，按指示将9900元学费转入对方账号...得知被骗，伤心欲绝，21日晕厥离世。(沂蒙晚报)网页链接



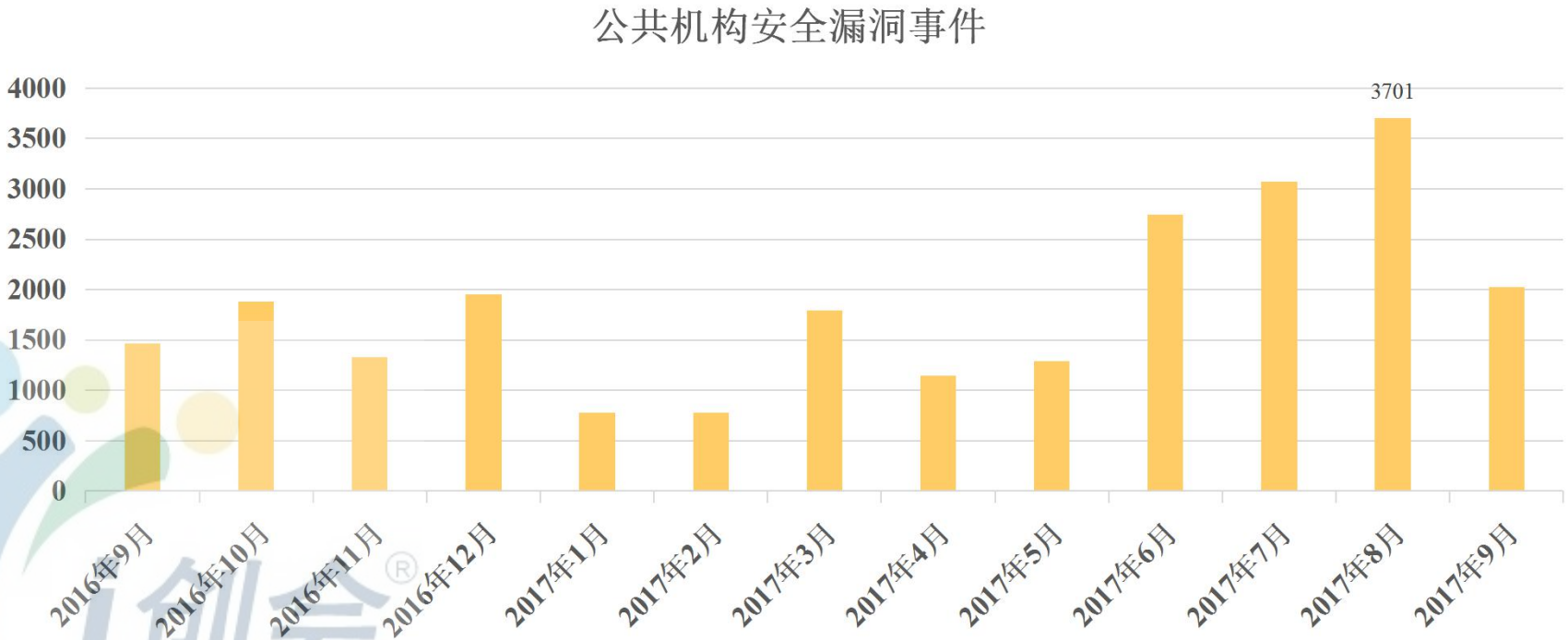


2016年8月，临沂女孩徐玉玉遭遇信息诈骗，不幸离世。此案件引起全国范围内广泛关注。这一悲剧的主要原因是信息泄露。“山东省高考网上报名系统”存在漏洞，泄露了包括徐玉玉在内64万名考生信息。

公共部门是被攻击重点

1. 政府部门、金融机构、医疗、教育等行业网站始终是不法分子攻击的重点目标。
2. 安全漏洞是公共部门信息系统遭攻击的主要原因，大多数是网站程序存在 SQL 注入、弱口令以及权限绕过等漏洞。
3. 政府网站被大量篡改、植入后门。
4. 金融、社会机构网站被大量仿冒。

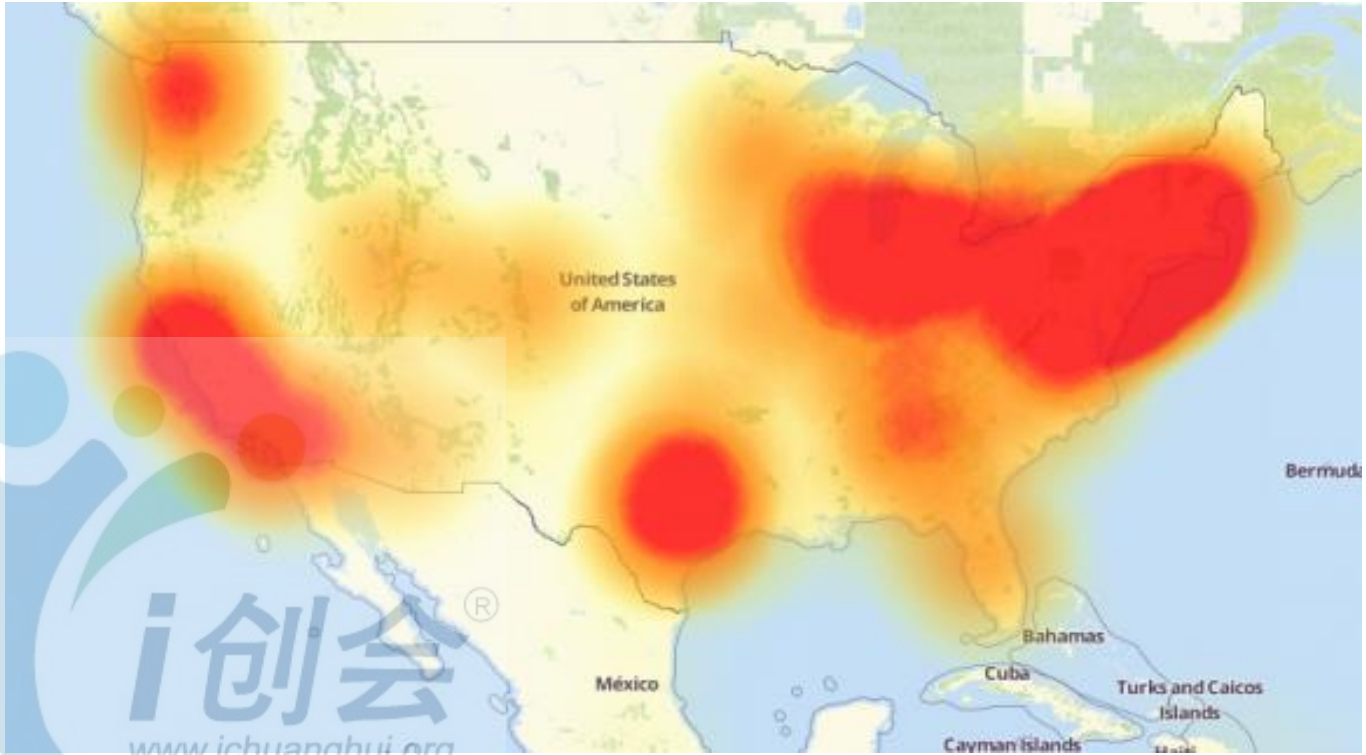
公共部门是被攻击重点（续1）



徐玉玉事件引起一系列网络安全变革

1. 2016年9月，央行、工信部、公安部、网信办等联合开展联合整治非法买卖银行卡信息专项行动。
2. 2016年12月，公安部延长打击整治网络侵犯公民个人信息专项行动。网信办统筹协调各相关部门开展打击整治行动。
3. 2016年12月，最高法、最高检、公安部共同发布的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》，网络诈骗最高无期。
4. 2017年，教育部开展网络安全综合治理行动，“治乱、补漏、补短、规范”。

二、“Mirai病毒”宣告僵尸物联网的到来

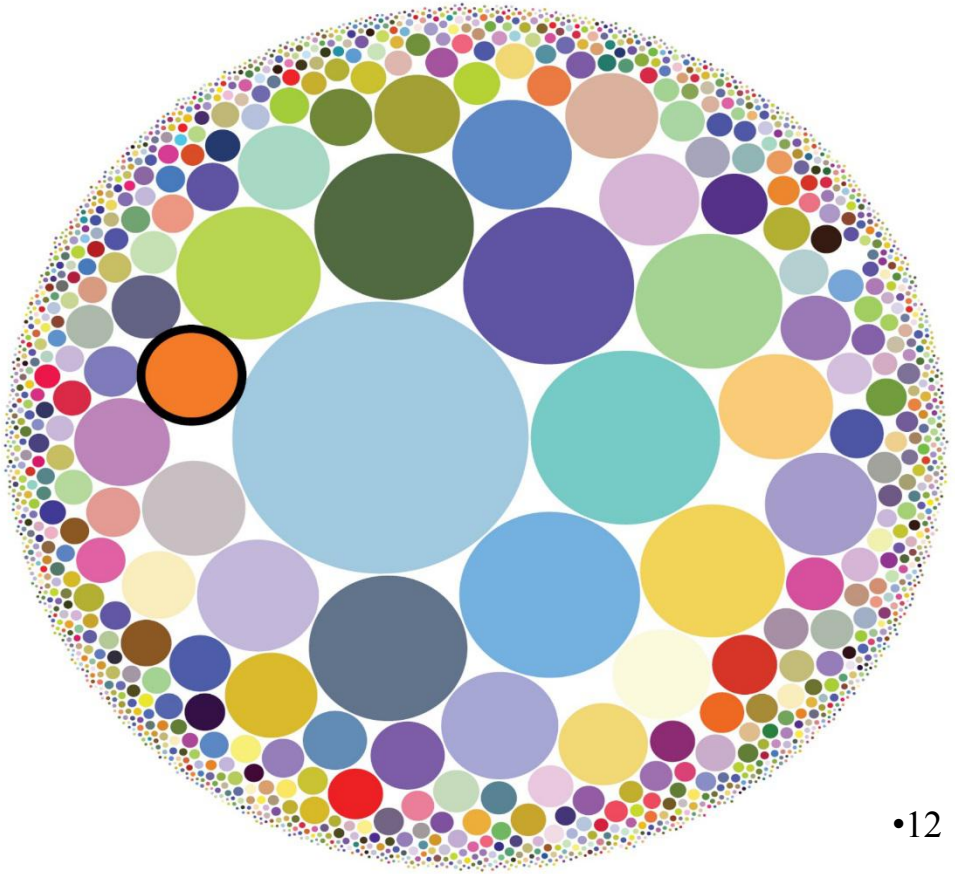


2016年10月，Mirai僵尸网络发起DDOS攻击导致半个美国互联网瘫痪。

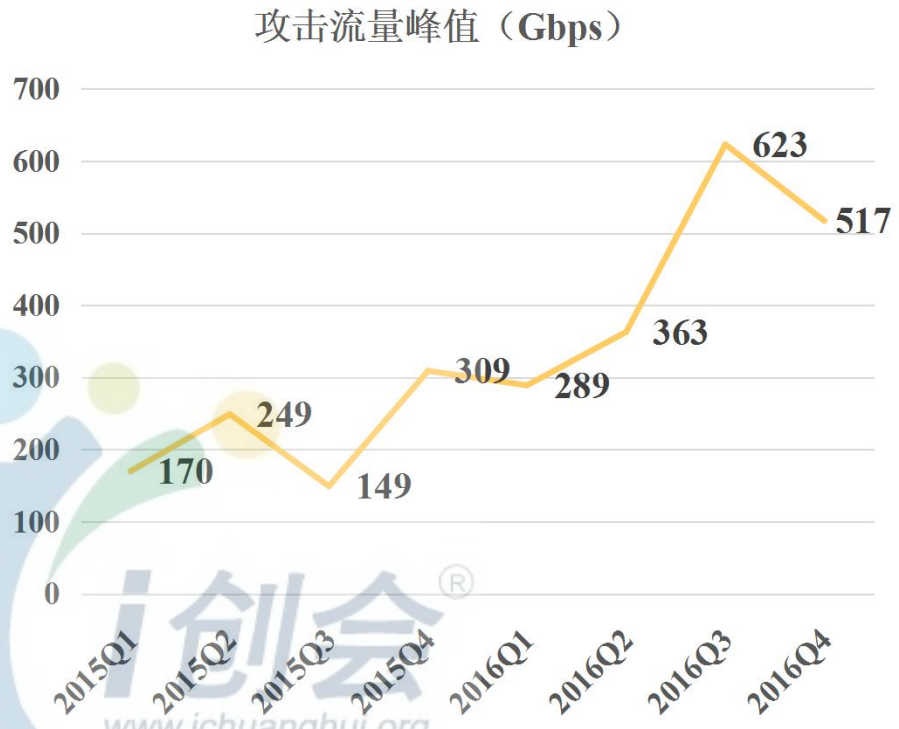
Mirai发起的DDoS攻击

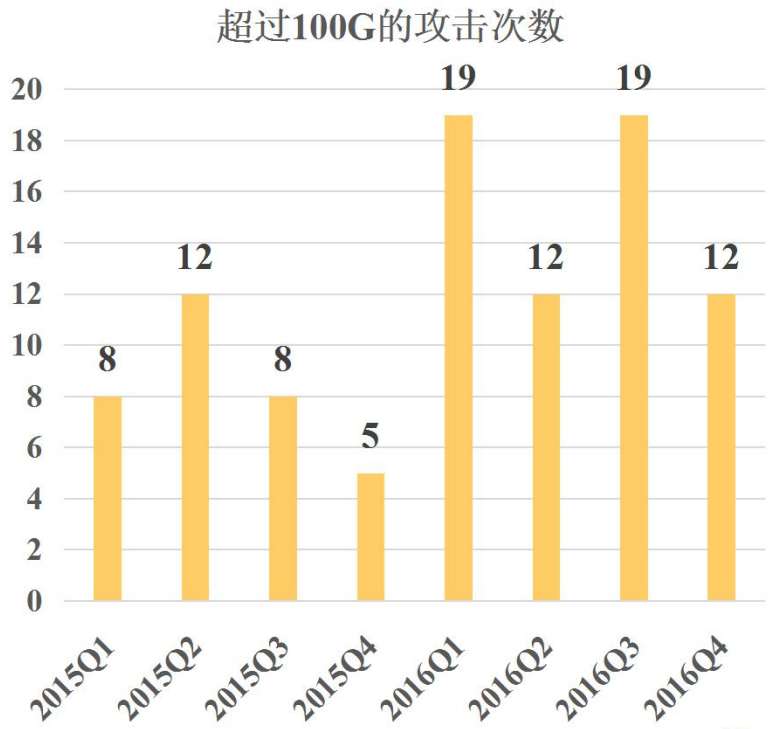
Akamai在《2017年第二季度互联网安全报告》中统计了Mirai发起的DDoS攻击。圆形代表被攻击目标。

Akamai被Mirai僵尸网络攻击了1246次，而最大受害者被攻击了10500次。

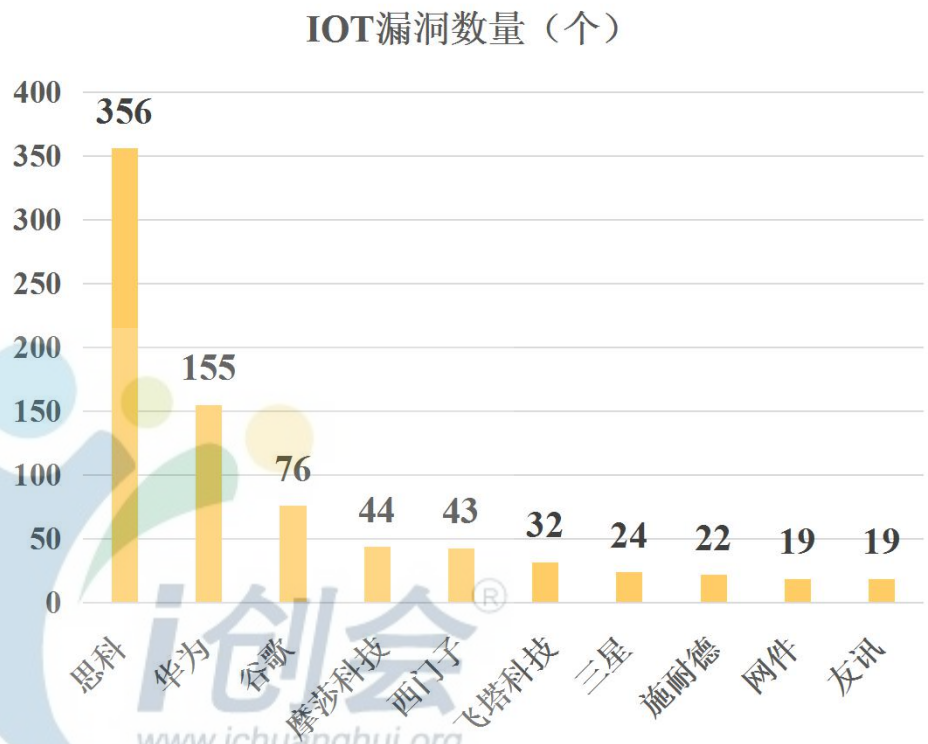


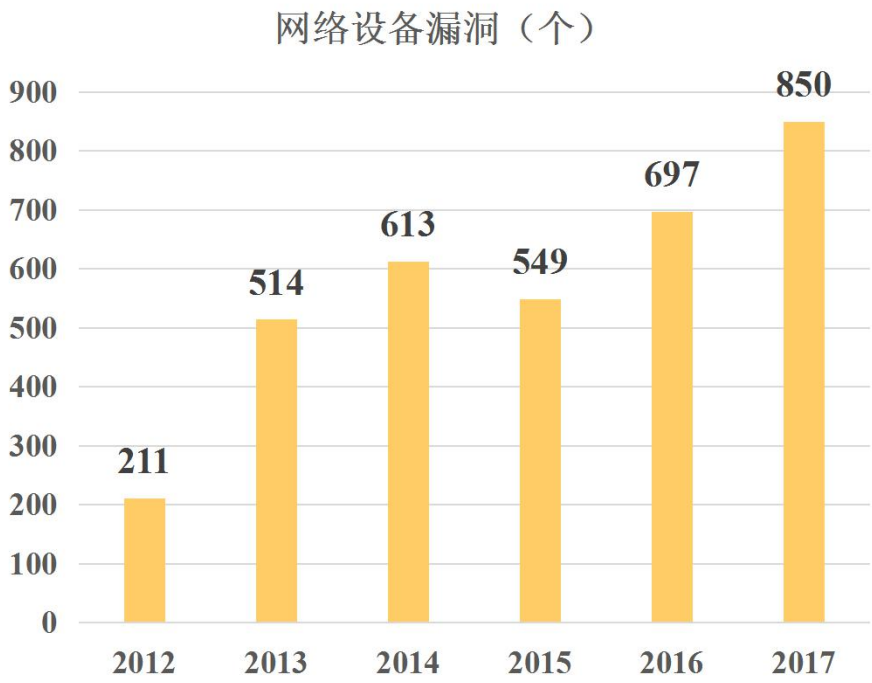
DDoS攻击爆发



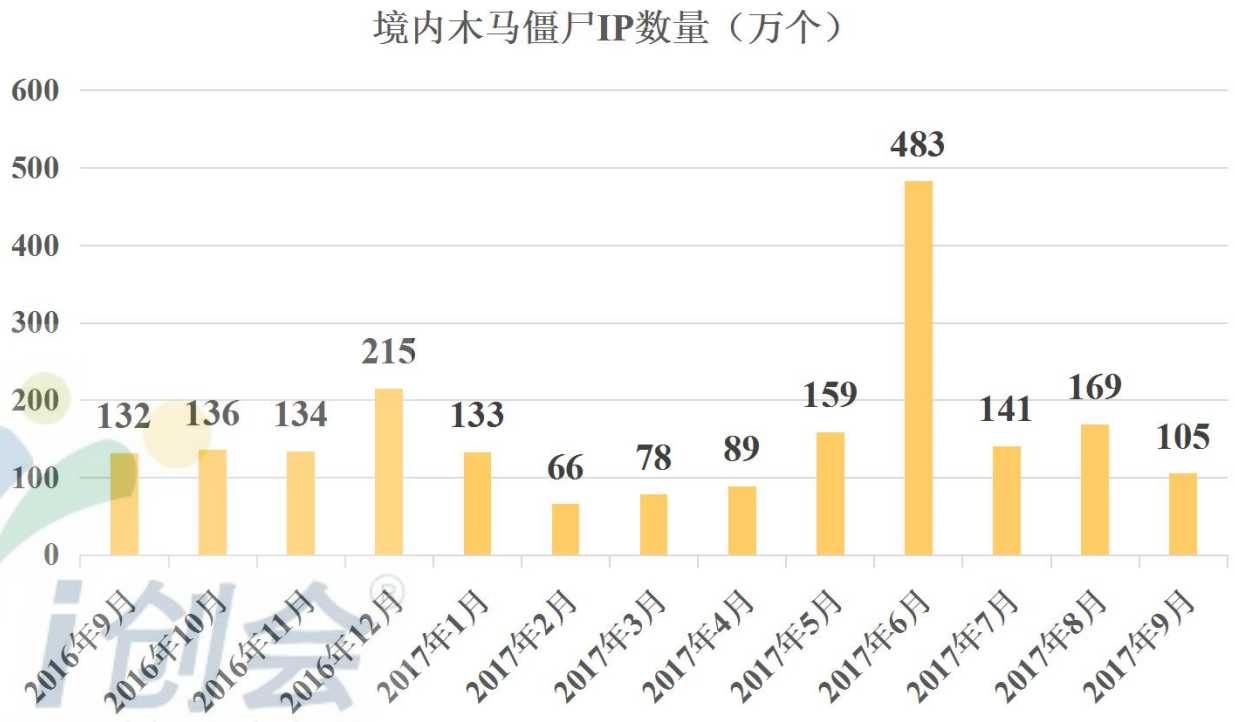


2016年CNVD收录1117个IoT漏洞





国内木马僵尸程序控制的IP地址



2017年6月，“暗云”木马在国内大量传播，控制了162万台主机，组成了超大规模的跨境僵尸网络。

僵尸物联网破坏大、难阻止

- 2017年2月，《麻省理工科技评论》把僵尸物联网列为2017全球十大突破性技术。僵尸物联网对互联网的破坏能力将会越来越大，也会越来越难阻止。
- 2017年9月，360捕获到脱胎于Mirai的恶意样本IoT_reaper。IoT_reaper已经感染了近200万台设备，并且每天增加10000台新设备。

三、“永恒之蓝”勒索病毒全球爆发

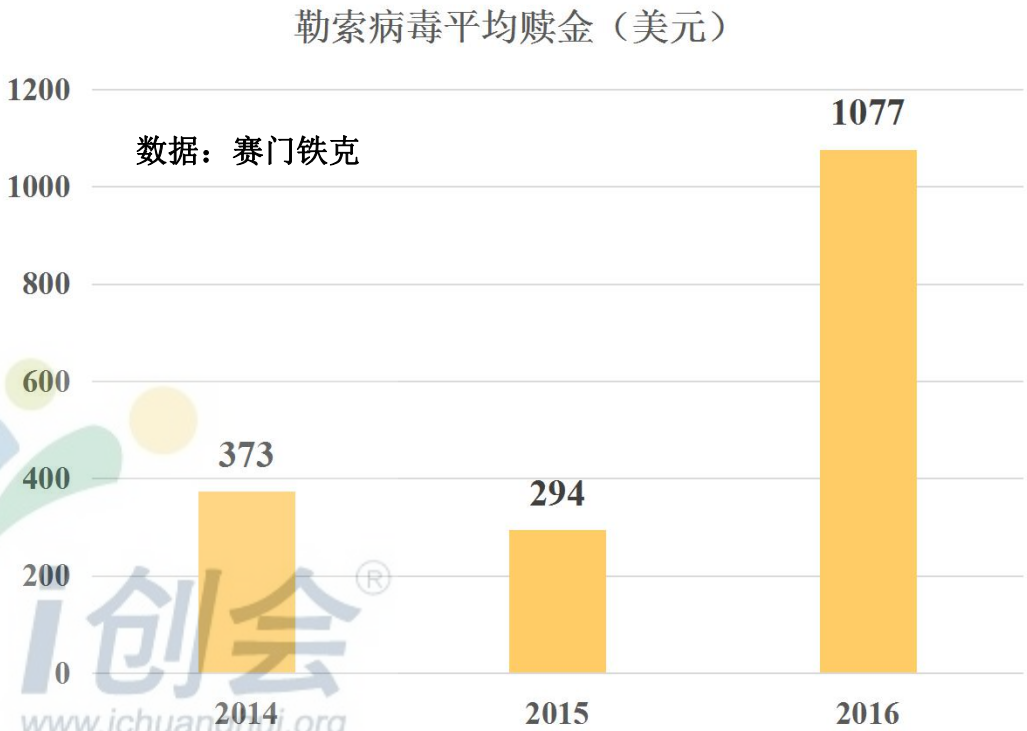
- 2017 年4月，影子经纪人（Shadow Brokers）公开了一大批NSA的黑客工具，包括永恒之蓝、永恒王者等可以远程攻破全球约70% Windows终端的漏洞利用工具。
- 2017年5月，针对永恒之蓝漏洞进行攻击的“想哭”勒索病毒在全球爆发，波及150多个国家和地区、10多万组织和机构，以及30多万网民，损失超过80多亿美元，部分机构因此次攻击瘫痪数月。

勒索病毒全球爆发（续1）

- 2017 年6月，勒索病毒Petrwrap病毒由乌克兰和俄罗斯开始爆发，迅速蔓延欧洲并席卷全球。其中，切尔诺贝利核电站设施也受到影响。

- 2017年10月底，新型勒索软件Bad Rabbit在东欧诸国爆发。乌克兰的一些交通组织以及一些政府组织遭受了网络攻击，导致一些计算机文件被加密勒索。

勒索病毒全球爆发（续2）



根据赛门铁克统计，2016年，全球爆发勒索事件46.4万次，平均每天发生1271次。

案件勒索额从294美元提升至1077美元。

四、掌握网络空间斗争主动权

- 当前我国在防御网络攻击方面，由于信息系统大量使用源代码不开放的专有操作系统而往往处于被动挨打的地位
- 首先是难以事先发现漏洞、预做准备。如使用Windows操作系统，不论是按早先的“源代码备案”协议（GSP），还是在目前“神州网信”合资公司，中方都看不到全部源代码，有数以百万行计的代码未对中方开放；而且代码的利用受严格限制，尤其是知识产权是属于人家的，导致中方广大安全工作者无法发挥作用。实际上，这类系统的漏洞只能等别人通知，或者当受到攻击后才被发现。
- 其次是由于缺乏研究条件以及没有知识产权，因而难以自打补丁，只能靠别人提供补丁；对所提供的补丁，也无法对其有效性进行正向评估，只能看实际结果，即“听天由命”。

发展自主操作系统的意义

- 基于开源软件发展自主操作系统，可以大大增强网络空间斗争的主动权。
- 可以事先发现漏洞，预做准备。只要有高水平的科技人员，进行深入的分析研究，完全可以事先发现漏洞，及时进行修补或预防。
- 发现漏洞或遭到攻击后，可以自打补丁；对发布的任何补丁都可以对其有效性进行评估，从而可以持续地改进安全性。
- 在条件成熟时，有可能提出创新的架构，发展出创新的安全操作系统，极大地提升系统的抗攻击能力。

实例——脏牛漏洞（Dirty Cow）（一）

- 漏洞简介：Linux内核存储子系统在处理写复制（COW）时出现一个竞争状态可破坏私有只读存储映射，一个非特权本地用户可利用这一漏洞获得对原先为只读存储映射的写权限，从而提升他们在系统中的权限。
- 该漏洞已存在很久，几乎影响 2007之后的所有Linux版本。但它又非常隐蔽，直到2016.10才被发现。这是因为 利用这一漏洞的攻击是通过操作系统的正常功能实现的，使常规病毒的检测方法无法发现。
- 使人们认识到掌握操作系统核心技术的重要性。即使是经过无数专家审查的那些开源软件，也存在着这类难以发现、可能产生重大后果的漏洞，至于那些源码不公开（或源码公开不充分/源码没有消化的）的软件，更无法保证不存在这类漏洞了。

2016.10.19国外权威网站发布了Dirty Cow漏洞消息

CVE-2016-5195

Impact: Important
Public Date: 2016-10-19
IAVA: 2016-A-0306

Bugzilla:1384344: CVE-2016-5195 kernel: mm: privilege escalation via MAP_PRIVATE COW breakage

A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged, local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

实例——脏牛漏洞（Dirty Cow）（二）

- 鉴于这一漏洞涉及到操作系统和信息安全两个领域的一些深层次问题，受到了业界的广泛重视。今年4月18日，中国网络空间协会（CSAC）在北京召开了一次操作系统漏洞研讨会，有来自各领域的80余名专家出席，就此漏洞及其相关问题进行了交流探讨。
- 会上，国科大杨力祥教授领衔的操作系统团队，基于多年来对Linux进行的深入研究和积累的丰富经验，向与会专家介绍了该漏洞的机理、对现有补丁的评估以及自行设计的补丁方案。
- 实际上，现在该漏洞的补丁是Linux的发明者Linus Torvalds本人所提供的。杨教授团队对其评估认为，这一补丁更多地着眼于效率，而并未完全消除竞争。他们团队则提出了一个变通的补丁方案，更多地着眼于安全，而在效率方面仅付出很小的代价。

实例——脏牛漏洞（Dirty Cow）（三）

- 杨教授团队认为，现存的操作系统不可避免地存在着类似于“Dirty Cow”这样的、具有严重危害的漏洞，因此他们认为需要发展一个能免除一切攻击（不包含拔去电源之类的人为破坏）的安全OS。
- 这一新系统将由新的OS、新的CPU和新的编译器组成一个统一的框架；新的CPU应为新的OS内核设置专门的安全指令；新的OS将基于专门的安全指令和新的OS架构；新的编译器将支持新的CPU和新的OS。
- 科技创新是发展网信事业（包括操作系统在内）的最大动力，我们希望杨教授团队和中国一切有志于操作系统和网络安全领域创新的团队，敢于创新，善于创新，脚踏实地，努力奋斗，尽快掌握网络空间斗争的主动权。

采用不同操作系统的网络安全效果评估

OS类型 / 网络安全评估	采用进口的专有OS（例如Windows）或合资公司的无自主知识产权、不掌握核心技术的OS	采用基于开源软件发展的自主OS（例如国产Linux OS）或自主发展的OS
是否能事先发现操作系统漏洞？	N	Y
是否能独立分析漏洞机理？	N	Y
是否能自打补丁？	N	Y
是否能深入评估补丁效果？	N	Y
是否能免除“后门”？	N	Y
是否有网络空间斗争主动权？	N	Y

五、加强网络法制建设

- 中国首部涉及网络安全的法规是《电子签名法》，这是为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益而制定的法律。自2005年4月1日起施行。
- 《中华人民共和国网络安全法》是我国这一领域的一部“基本法”，已自2017年6月1日起施行。
- 依据《国家安全法》、《网络安全法》等法律法规，国家互联网信息办公室发布了《网络产品和服务安全审查办法》，已自2017年6月1日起施行。
- 有关网络安全的其他许多法规制度也正在继续制订完善中。

中国的信息安全等级保护制度

- 信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。
- 重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统。
- 信息安全等级保护是当今发达国家保护关键信息基础设施、保障信息安全的通行做法，也是我国多年来信息安全工作经验的总结，事关国家安全、社会稳定、国家利益的重要任务。

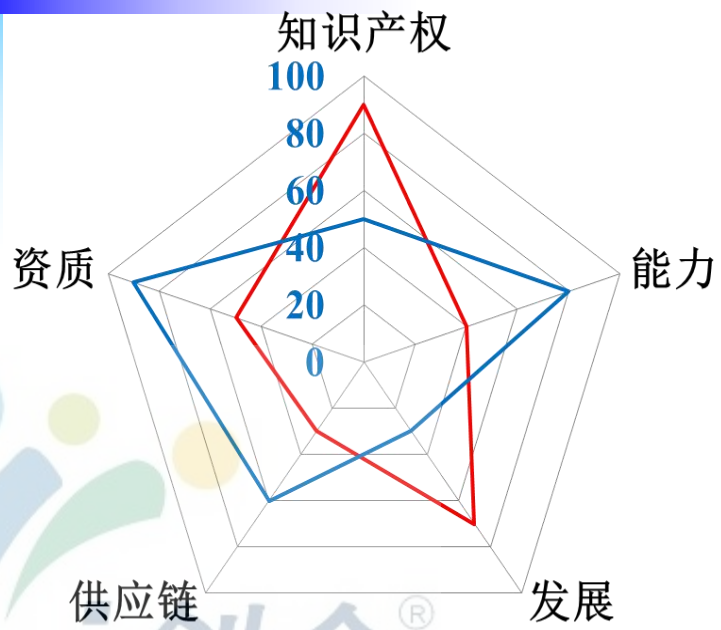
中国的信息安全等级保护制度（续1）

- 信息系统的安全保护等级根据其重要性从低到高分为五级；相应地，计算机信息系统安全保护等级划分为以下五级：
  - 第一级：用户自主保护级；
  - 第二级：系统审计保护级；
  - 第三级：安全标记保护级；
  - 第四级：结构化保护级；
  - 第五级：访问验证保护级。
- 等保是针对非涉密网而言，由公安部门发起，坚持自主定级、自主保护原则；对于涉密信息系统实行分级保护（分三级），由国家保密局发起，是强制性的，是等级保护在涉密领域的具体体现。
- 我国信息安全等级保护制度在实践中已经取得了良好的效果。

多维度测评

- 在网络安全范畴中“安全”的内涵与传统领域中“安全”的内涵有所不同。实际上，前者的内涵更大、更广，例如自动驾驶汽车的“安全”性不仅包含了传统汽车的“安全”性，还包含了能抵御网络攻击、能保护用户信息等等，所以需要评估“安全性”和“可控性”。
- 为此，有关部门提出了实行多维度测评的要求：
  - **自主可控评估**——对产品/服务/系统的自主可控性进行评估，这种评估可以是针对CPU、操作系统等核心技术产品，也可以针对一个信息系统或一项信息基础设施。
  - **质量测评**——对产品/服务/系统的功能、性能等等技术指标进行测评；
  - **安全测评**——对产品/服务/系统的安全性进行测评，这种测评有可能与“等保”、“分保”的测评相结合。

自主可控评估的一种方案



图示的自主可控评估方案，比较适合CPU、OS这类产品，如果是对云计算、大数据等云服务，除评估这些指标外，还应重点评估：

- 所用软硬件是否自主可控？
- 基础设施是否部署在境内？
- 敏感信息是否不出境？
- 用户隐私信息是否不泄露？
- 是否能防御网络攻击？
- ……

1. 知识产权（包括标准）自主可控

- 在当前的国际竞争格局下，知识产权自主可控十分重要，做不到这一点就一定会受制于人。如果所有知识产权都能自己掌握，当然最好，但实际上不一定能做到，这时，如果部分知识产权能完全买断，或能买到有足够自主权的授权，也能满足自主可控。
- 然而，如果只能买到自主权不够充分的授权，例如某项授权在权利的使用期限、使用方式等方面具有明显的限制，就不能达到知识产权自主可控。
- 目前国家一些计划对所支持的项目，要求首先通过知识产权风险评估，才能给予立项，这种做法是正确的、必要的。标准的自主可控似可归入这一范畴。

2. 技术能力自主可控

- 能力自主可控，主要指技术能力的自主可控，这意味着要有足够规模的、能真正掌握该技术的科技队伍。
- 技术能力可以分为一般技术能力、产业化能力、构建产业链能力和构建产业生态系统能力等层次。产业化能力的自主可控要求使技术不能停留在样品或试验阶段，而应能转化为大规模的产品和服务。产业链的自主可控要求在实现产业化的基础上，围绕产品和服务，构建一个比较完整的产业链，以便不受产业链上下游的制约，具备足够的竞争力。产业生态系统的自主可控要求能营造一个支撑该产业链的生态系统。

3. 发展主动权自主可控

- 除了知识产权和能力的自主可控，还需要有发展的自主可控，因为我们不但要着眼于现在，还要求在今后相当长的时期里，对相关技术和产业而言，都能不受制约地发展。
- 为此，根据我国具体情况，要着眼国家安全和长远发展，制订信息核心技术设备的发展战略。如果某些技术在短期内似乎能自主可控，但长期看做不到自主可控，一般说来是不可取的。只顾眼前利益，有可能会在以后造成更大的被动。

4. 供应链自主可控

- 一个产品的供应链可能很长，如果其中的一个或某些环节不能自主可控，也就不能满足自主可控要求。例如对复杂的CPU芯片来说，即使拥有知识产权，也有技术能力掌握，做到在设计方面不受制于人，但如需依赖外国才能进行生产，那么仍然达不到自主可控的要求。
- 所以，应当评估一个产品的供应链是否能完全掌控？像上述复杂的CPU芯片，如果必须依赖外国进行生产加工，就不能满足自主可控的要求。如果能够依靠本国厂商生产出来，即使性能指标略低一些，还是可以容许的。

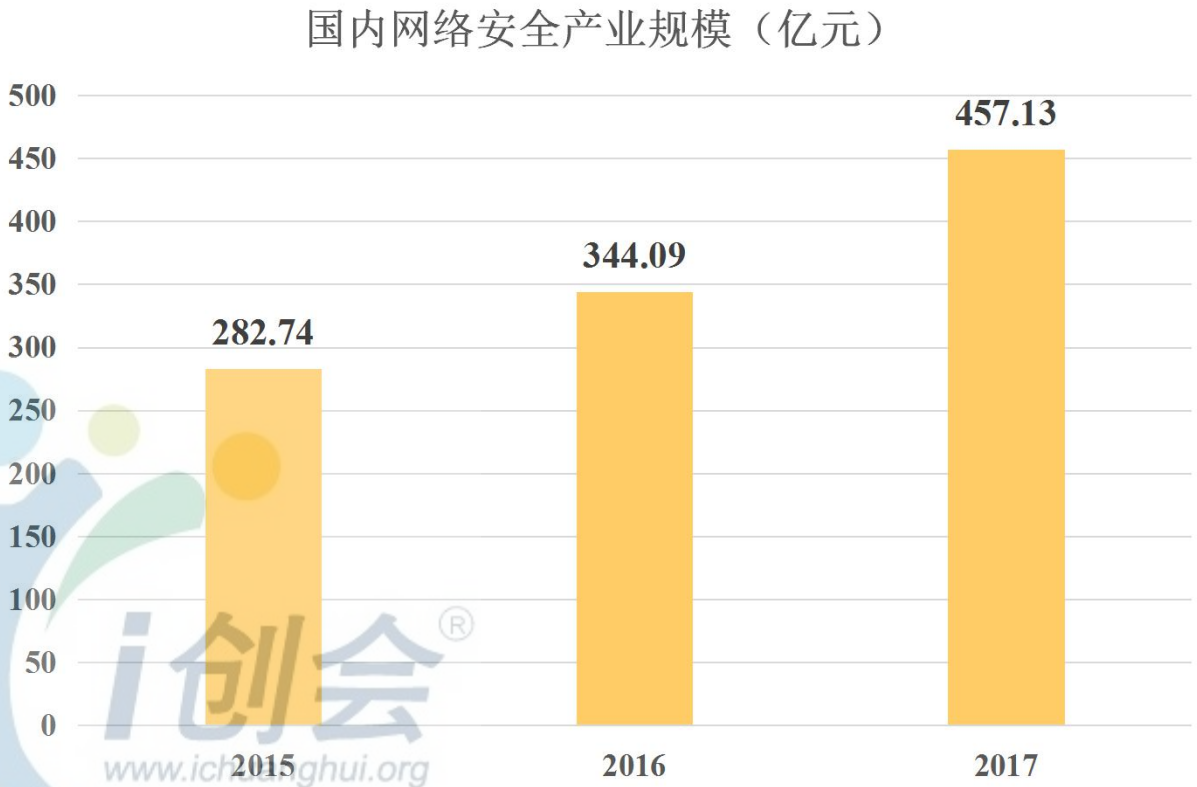
5. “国产”资质和本土增值

- 一般说来，“国产”产品和服务容易符合自主可控要求，因此实行国产替代对于达到自主可控是完全必要的。不过现在对于“国产”还没有统一的评估标准。
- 过去有人提出的某些评估标准显然是不合适的。例如：认为只要公司在中国注册、交税，就是“中国公司”，它的产品和服务就是“国产”；或认为“本国产品是指在中国关境内生产，且国内生产成本比例超过50%的最终产品”。这里，突出“生产成本”完全不适用于高技术领域。众所周知，高技术产品和服务的成本主要是开发成本、智力成本，生产成本甚至可以忽略不计，这种“生产成本”准则是帮进口高技术产品的忙，因为它们只要用中国原材料做个包装，就可以摇身一变成为“国货”了。

“国产”资质和本土增值（续1）

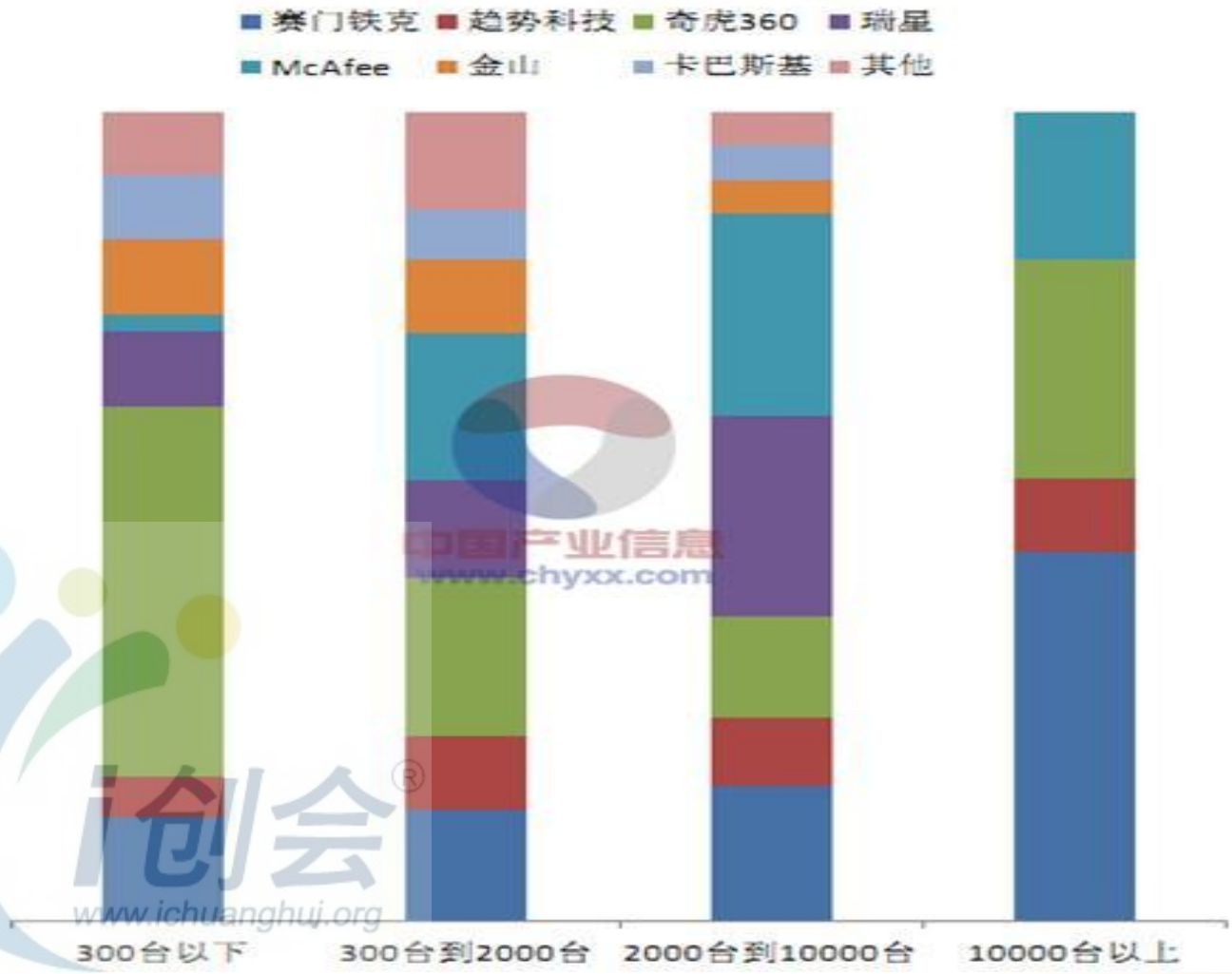
- 美国国会在1933年通过的《购买美国产品法》，要求联邦政府采购要买本国产品，即在美国生产的、增值达到50%以上的产品，进口件组装的不算本国产品。美国采用上述“增值”准则来评估“国产”，比较合理。这方面我们理应学习发达国家行之有效的做法。
- 对于“国产”的评估，我们主张除了考察资质外，还应采用“增值”准则对“国产化程度”加以评估，因为如某项产品和服务在中国的增值很小，意味着它可能就是从国外进口的，达不到自主可控要求。如果实行“增值”估算，“贴牌”、“穿马甲”之类的“假国产”就难以立足了。
- 综上所述，制订自主可控的评估标准是可行的，有助于加快发展自主可控的信息技术和产业，贯彻落实国家网络安全有关法规。

六、中国信息安全产业发展状况



网络安全市场：

根据中国信息通信研究院统计测算，2016 年我国网络安全产业规模约为 344.09 亿元，较 2015 年增长 21.7%，预计 2017 年达到 457.13 亿元。



防病毒软件发展状况：

目前国外厂商在大企业市场拥有优势。赛门铁克、趋势科技和 McAfee占据了最大市场份额。近年来，国产厂商奇虎360、瑞星、金山等发展较快。

中国防病毒软件发展面临垄断的制约

- 作为发展中国家，中国防病毒软件企业的发展受到占据垄断地位的跨国公司的制约，尤其是Win10绑定了微软可信技术和Defender防病毒软件，使第三方防病毒软件不能发挥作用，随着Win10市场份额的不断扩大，它们的前景堪忧。
- 希望有关方面能根据反垄断法的规定，仿照当年欧盟要求微软从Windows中剥离IE的做法，要求微软提供剥离了其可信技术和Defender的Win10版本，使用户有更多的防病毒软件选择，使第三方防病毒软件企业有生存的机会。
- 在维护网络安全方面，“不能一个国家安全而其他国家不安全，一部分国家安全而另一部分国家不安全”。各国都有发展防病毒技术的权利，市场垄断者不能滥用市场支配地位限制别国发展防病毒技术。

谢谢大家！