网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

内部资料

关于网络安全态势感知研判工作的一些思考

中国网络空间安全协会 副秘书长
天津理工大学网络空间安全研究院 院长
张健

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰

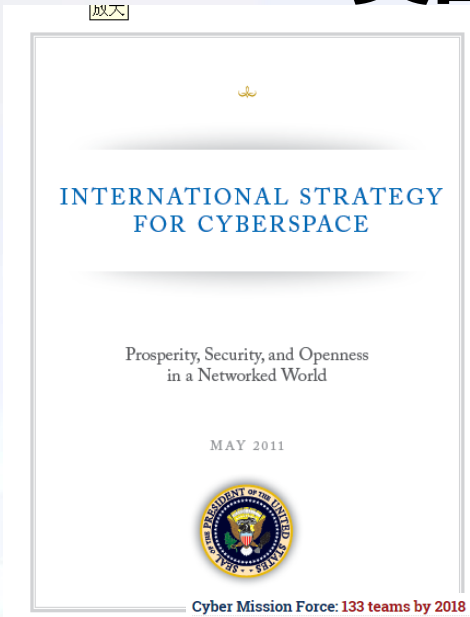
提纲

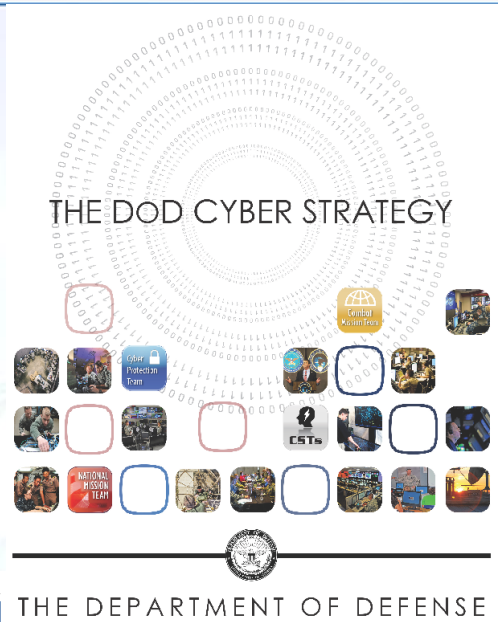
- 网络安全形势严峻复杂
- 网络安全态势感知研判工作
- 态势感知工作的一些思考

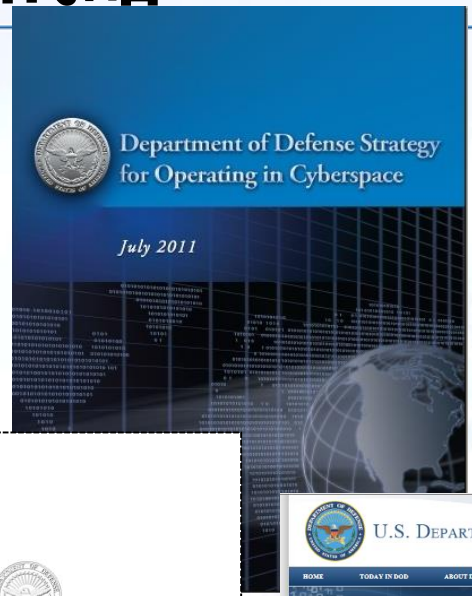
01 网络安全形势严峻复杂

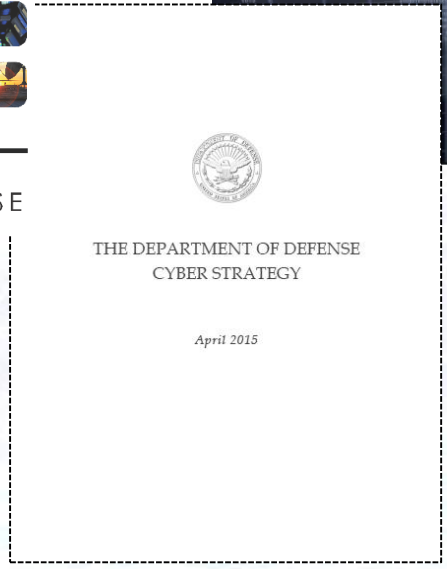
一、网络空间剑拔弩张

美国发布一系列网络空间战略









美国发布一系列网络空间战略（续）

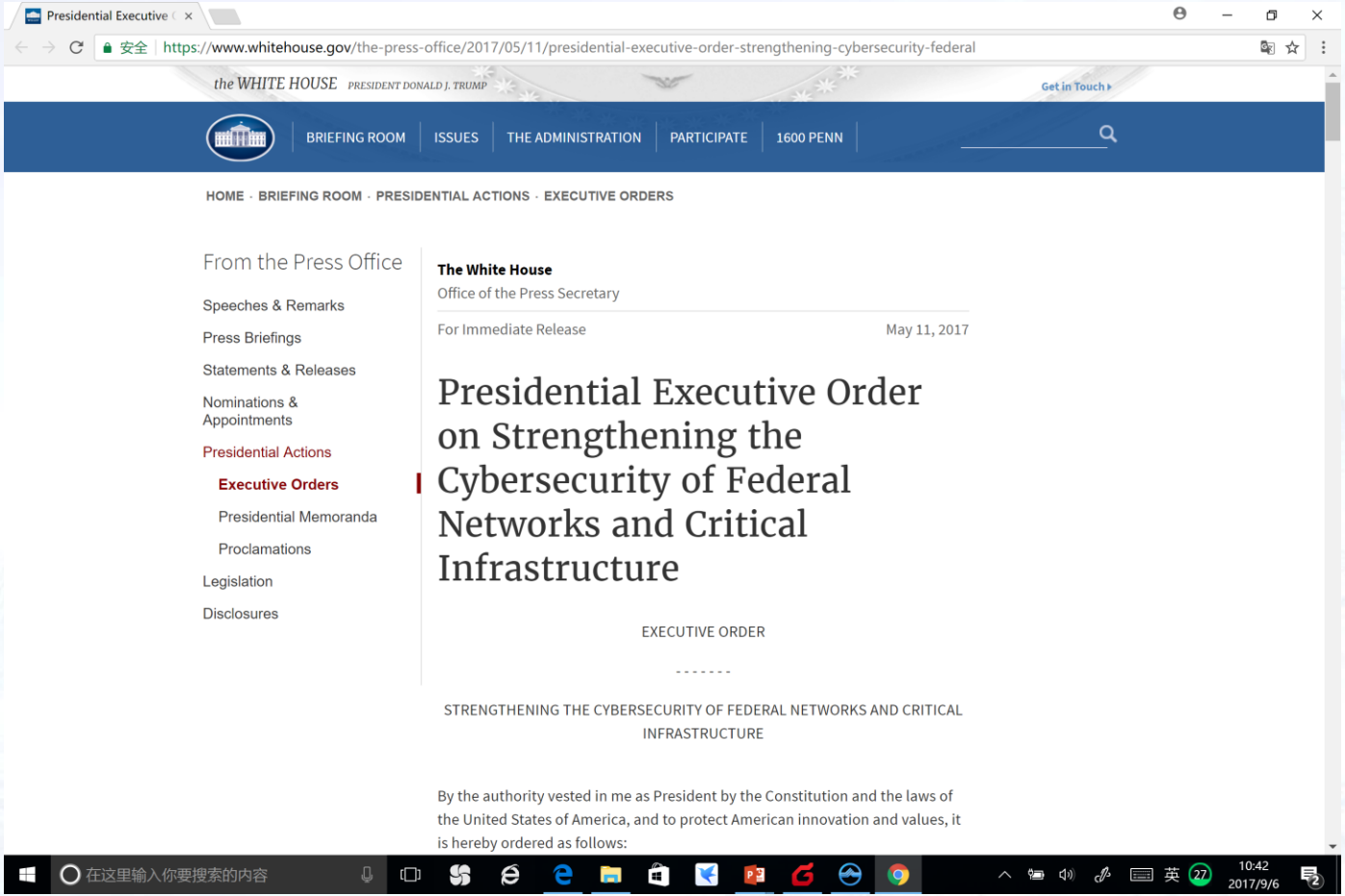
- 2011年5月16日，白宫、 国务院、司法部、商务部、国土安全局、国防部这六个美国联邦政府部门共同发布了《网络空间国际战略》（international strategy for cyberspace） 。美国视互联网、太空和海洋为全球公地。和其它两个公地一样，美国要确保在网络空间的战略威慑力。
- 2011年7月14日，美国防部在其网站上发布了首份《网络空间行动战略》部分内容，新战略包括进一步将网络空间列为与陆、海、空、太空并列的“行动领域”。美军已经将网络空间的威慑和攻击能力提升到更加重要的位置。
- 2015年4月，美国防部第二次发布《网络战略》。确定三大任务：
- 一是防卫国防部的网络、系统和信息；
- 二是保卫美国国土及国家利益不受重大网络袭击活动的侵犯；
- 三是集中网络军队力量支持军事行动和应急计划。
- 2015年，美国发布了《网络安全法》。
- 2015年12月，白宫向美国会提交了《网络威慑战略》文件。
- 2016年2月，美国发布了“网络安全国家行动计划(CNAP)”。

特朗普签署《增强联邦政府网络与关键性基础设施网络安全》行政令

- 2017年5月11日，特朗普签署《增强联邦政府网络与关键性基础设施网络安全》。该行政指令要求各联邦政府机构在90天内制定风险管理报告，并提交给国土安全部部长和白宫行政管理与预算办公室主任，描述该机构如何实施由美国国家标准技术研究所（NIST）制定的提升关键基础设施网络安全框架。在收到报告60天内，行政管理与预算办公室主任应通过负责国土安全和反恐事务的总统国家安全事务助理，向总统提交对各机构风险管理报告的评估意见及实施计划。此外，以建立一个“现代、安全、更有韧性”行政部门信息技术架构为目标，美国技术委员会主任应在90天内向总统提交各部门的转型情况。国防部和情报系统等国家安全系统则应在150天内向负责国土安全和反恐事务的总统国家安全事务助理提交有关实施情况的报告。
- 在关键基础设施网络安全方面，要求按奥巴马政府时期颁布的第21号总统行政指令中所规定的关键基础设施名单，对之进行评估，并于180天内提交网络安全风险评估报告，随后每年提交一次评估报告。

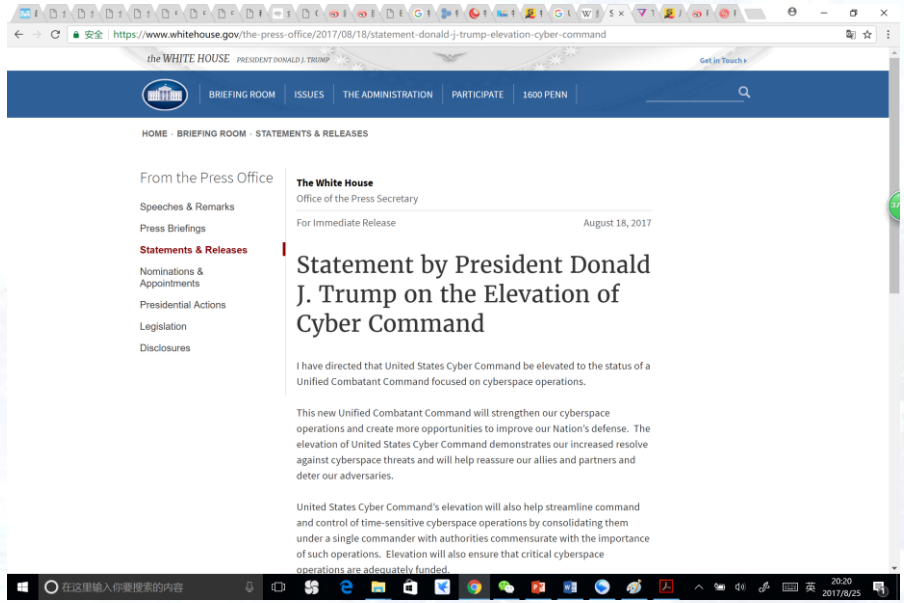
•“To truly make America safe, we truly have to make cybersecurity a major priority.”
Then-candidate Donald Trump on October 3, 2016

特朗普签署《增强联邦政府网络与关键性基础设施网络安全》行政令（续）

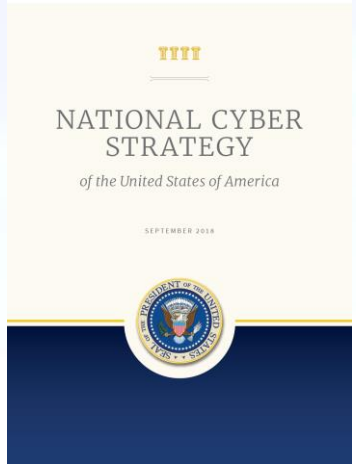


美国网络司令部升格

- 2017年8月18日，美国总统唐纳德·特朗普批准了一项将美国网络司令部(Cyber Command)从美国国家安全局（NSA)分离的计划。网络司令部将升级为最高级别联合作战司令部(Unified Combatant Command)。这将使网络司令部与美国现有其他9个联合作战司令部“平起平坐”，在处理网络空间业务时，增加其独立性。



2018年9月20日，美发布《国家网络战略》



一、 保护美国人民、国土及美国人的生活方式

目标：管控网络安全风险，提升国家信息与信息系统的安全与韧性

（一） 保护联邦网络与信息

（二） 保护关键基础设施

（三）打击网络犯罪，完善事故报告制

二、 促进美国的繁荣

目的:维护美国在科技生态系统和网络空间发展中的影响力。

（一） 培育一个充满活力和弹性的数字经济

（二） 培育和保护美国的创造力

（三） 培养优秀的网络安全人才

三、 以实力求和平

目标：识别、反击、破坏、降级和制止网络空间中破坏稳定和违背国家利益的行为，同时保持美国在网络空间中的优势。

（一） 通过负责任的国家行为规范增强网络稳定性

（二）对网络空间中的不可接受的行为进行归因和威慑，在美国促进负责任国家行为共识的同时，还必须确保不负责任的行为将会有严重的后果，对此，***应利用所有的国家权力工具来防止针对美国的恶意网络活动，包括外交、军事、财政、情报、公开归因和执法能力等***，并与志同道合的伙伴国联合行动。优先行动主要有4项:（1）情报领先，确保情报部门在全源网络情报的使用上处于世界领先地位，以推动对恶意网络活动进行甄别和归因。美国政府和主要合作伙伴将共享客观和可操作的情报以确定敌对国和非国家的网络行动意图、能力、研究和活动。（2）“后果”明确，美国将发展快速、公开和潜在的后果措施，以遏制潜在的恶意行为者。（3）构建网络威慑倡议，美国将启动一项国际网络威慑倡议，以联合志同道合的国家，协调对重大恶意网络事件的回应，包括通过情报共享、支持归因声明与回应行动，以及联合对恶意行为者施加后果。（4）***反恶意网络影响和信息行动，美国将使用所有国家权力工具来揭露和反击网络恶意影响和信息运动以及虚假信息的泛滥，识别、对抗和防止外国利用数字平台进行有害的信息活动。***

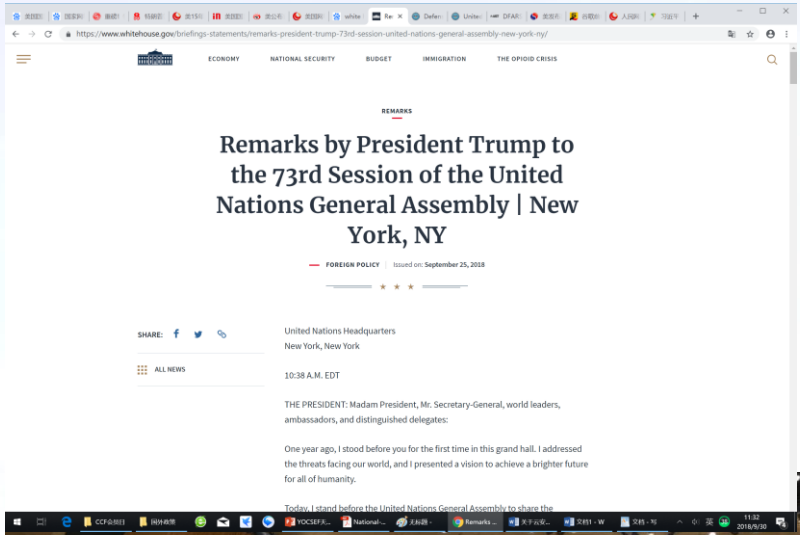
四、 扩大美国影响力

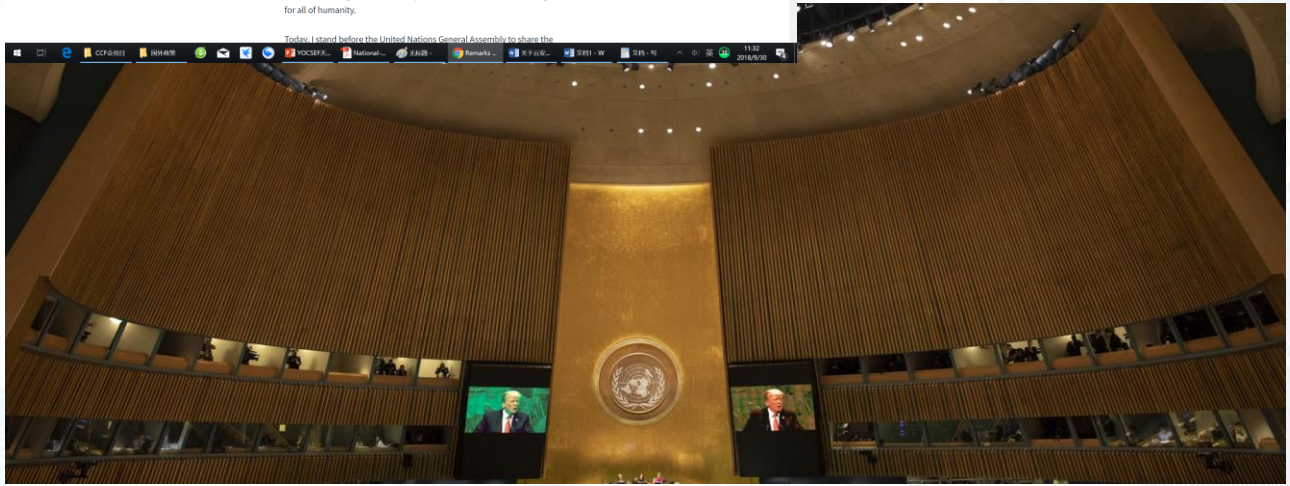
目标:保持互联网的长期开放性、互操作性、安全性和可靠性。

（一）促进开放、互操作、可靠和安全的互联网

（二）建设国际网络能力

特朗普联合国大会演讲表现如何？美媒集体给“差评”





二、网络空间治理博弈加剧

全球网络空间治理博弈加剧

- 美国关于网络空间的“全球公域说”就是建立在自由主义理念之上的，这种观点认为网络空间是全人类共享的空间，没有主权，私营部门和全球公民社会应当在网络空间治理中发挥主导作用。
- “多利益攸关方模式”。以美国为代表的西方网络强国主张由技术专家、商业机构和民间团体来主导网络空间治理，政府不应该过多干预，甚至国家间政府组织例如联合国也应该被排除在外。
- “多边主义模式”。发展中国家更倾向于政府主导，主张通过联合国等国际组织加强网络空间治理。
- 网络强国特别是美国坚持“多利益攸关方模式”的目的在于否定政府的作用，否定网络主权，而发展中国家坚持政府主导型的“多边主义模式”则是以网络主权为基础的。

金砖国家领导人厦门宣言

- 56. 我们支持联合国在制定各方普遍接受的网络空间负责任国家行为规范方面发挥中心作用，以确保建设和平、安全、开放、合作、稳定、有序、可获得、公平的信息通信技术环境。我们强调《联合国宪章》确立的国际法原则至关重要，特别是国家主权、政治独立、领土完整和国家主权平等、不干涉别国内政、尊重人权和基本自由。我们强调应加强国际合作，打击滥用信息通信技术的恐怖主义和犯罪活动，重申德班宣言、福塔莱萨宣言、乌法宣言和果阿宣言为此提出的建议。正如乌法宣言提及，应在联合国主导下制定国际法律文书以打击使用信息通信技术的犯罪行为。我们满意地注意到金砖国家关于信息通信技术使用安全性专家工作组取得的进展。我们决定根据《金砖国家确保信息通信技术安全使用务实合作路线图》或者任何其他达成共识的机制推进合作，注意到俄罗斯关于金砖国家达成确保信息通信技术安全使用的政府间合作协议的倡议。

三、网络犯罪活动高发

网络犯罪已成为第一大犯罪类型

- 全国社会治安综合治理表彰大会于2017年9月19日至20日在北京举行。中共中央政治局委员、中央政法委书记孟建柱说，**现在网络犯罪已成为第一大犯罪类型；未来绝大多数犯罪都可能借助网络实施。**我们要打破以传统办法对付网络犯罪的思维定式，深入研究网络黑灰产业链产生蔓延特点，完善全产业、全链条打击整治机制，提高线索发现、全程追溯、证据固定、依法打击能力，以立体防控链摧毁犯罪产业链，坚决把网络犯罪高发态势压下去。
- 孟建柱说，去年以来，通过综合治理，电信网络诈骗犯罪得到有效遏制，但不法分子与我打“游击战”，将窝点转移至世界各地。我们要坚持侦查打击、重点整治、规范治理“三管齐下”，发挥好电信、银行等部门的重要作用，堵住诈骗电话入境、诈骗赃款出境通道。深化执法司法国际合作，推动铲除境外窝点，依法追缴通过地下钱庄等流向境外赃款，最大限度维护受害人合法权益。
- 孟建柱还指出，前不久，150多个国家和地区网络用户陆续遭到新一轮勒索病毒攻击，标志着世界网络安全和网络战进入新阶段。我们要树立主动防御的理念，建立与国家关键信息基础设施面临威胁相适应的网络安全综合防御体系。

网络盗窃活动猖獗

孟加拉央行攻击事件

- 2016年2月5日，孟加拉国央行（Bangladesh Central Bank）被黑客攻击导致8100万美元被窃取，攻击者通过网络攻击或者其他方式获得了孟加拉国央行SWIFT系统操作权限，进一步攻击者向纽约联邦储备银行（Federal Reserve Bank of New York）发送虚假的SWIFT转账指令，孟加拉国央行在纽约联邦储备银行上设有代理帐户。纽约联邦储备银行总共收到35笔，总价值9.51亿美元的转账要求，其中30笔被拒绝，另外5笔总价值1.01亿美元的交易被通过。进一步其中2000万美元因为拼写错误（Foundation误写为fandation）被中间行发觉而被找回，而另外8100万美元则被成功转走盗取。
- 而我们捕获到的这次网络攻击中所使用的恶意代码，其功能是篡改SWIFT报文和删除相关数据信息以掩饰其非法转账的痕迹，其中攻击者通过修改SWIFT的Alliance Access客户端软件的数据有效性验证指令，绕过相关验证。

非法“挖矿”严重威胁互联网网络安全

- 非法“挖矿”严重威胁互联网网络安全。多家互联网企业和网络安全企业分析认为，非法“挖矿”已成为严重的网络安全问题。其中，腾讯云监测发现，随着“云挖矿”的兴起，云主机成为挖取门罗币、以利币等数字货币的主要利用对象，而盗用云主机计算资源进行“挖矿”的情况也显著增多;知道创宇安全团队监测发现，“争夺矿机”已成为僵尸网络扩展的重要目的之一;360企业安全技术团队监测发现一种新型“挖矿”病毒(挖取XMR/门罗币)，该病毒在两个月内疯狂传播，非法“挖矿”获利近百万元人民币。

恶意软件数量激增

各类网络敲诈勒索活动频发

“敲诈者”木马-2006年6月

全国首例计算机病毒网络敲诈案在广州告破

http://www.sina.com.cn 2006年07月25日 10:15 南方日报

广州网警发现某电脑公司一名技术总监沦为敲诈者

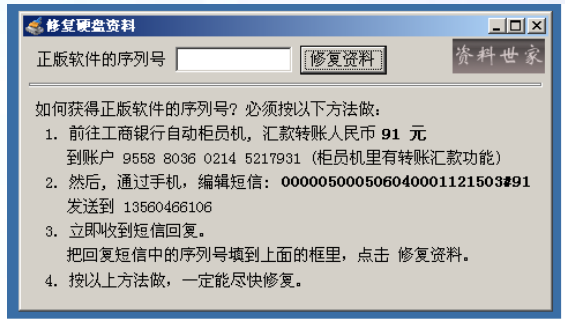
本报讯 （记者/刘中元 实习生/简玲珠 通讯员/陈立雄 张毅涛 翟光平）昨天，记者从广州市公安局新闻办获悉：广州市公安局网监分局近日侦破全国首例制作计算机病毒实施网络敲诈案。

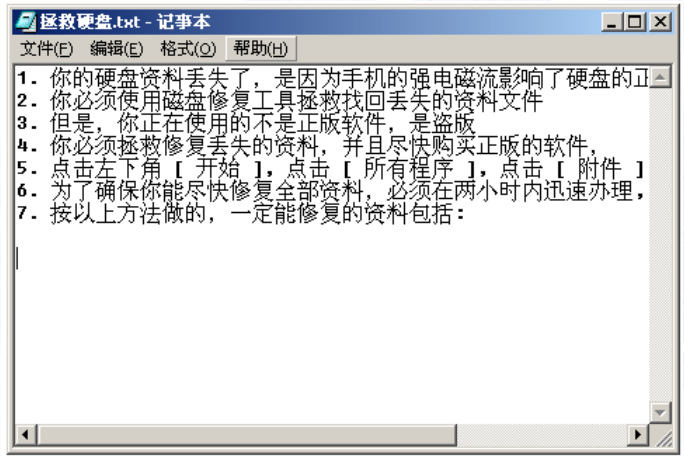
7月3日晚上9时许，犯罪嫌疑人欧阳××在人民北路露面，民警迅速将其抓获。同时，民警在欧阳××位于白云区某住宅小区的房间内当场查获作案工具计算机2台及手机卡、银行卡一批。

“敲诈者”放毒，“拯救硬盘”勒索

从6月14日开始，广州公安局网监分局陆续接到群众报案称，他们的电脑中出现一种名为“敲诈者”的新型电脑木马病毒。所有中招者受害路径如下：在“新曦数据库”网站下载企业资料后，电脑立即中毒，从而导致硬盘内公司资料丢失；等到重启电脑后，电脑桌面就会出现一名为“拯救硬盘”的TXT文件，等机主执行该文件后，电脑会自动出现一界面，它要求用户通过银行柜员机转账50元到99元不等，然后通过手机编发短信发送至特定号码，根据回复短信中的序列号即可修复硬盘资料。

据介绍：这种病毒可在短期内生出7个变种，经运行后，能恶意隐藏计算机用户系统中的文档，同时，系统里会出现可帮助计算机用户修复丢失掉的数据信息的文本文件“拯救磁盘.txt ”。





“敲诈者”木马制造者

据国家计算机病毒应急及处理中心透露:至今年6月29日为止，共接到“敲诈者”病毒感染报告450例，传播范围遍及全国。

现实敲诈者，曾是网络技术总监

专案组民警根据互联网上的线索，查到病毒制造者的真实身份。

据了解，欧阳××今年34岁，广州人，1999年从广州某大学金融证券专业毕业，曾经在一些电脑公司担任过网络技术员、技术总监，2003年至今是自由职业者。

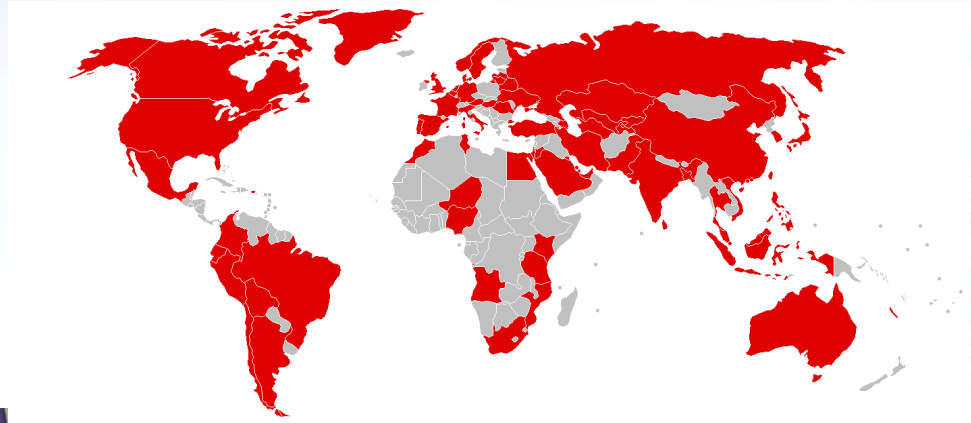
他平时爱好电脑编程，并在互联网上开设有个人网站。今年以来，因经济上入不敷出，他于是产生利用病毒程序赚钱的想法。

今年6月7日至6月24日期间，他制作出计算机病毒程序，并放置病毒程序在其个人网站“新曦数据库”公布的企业信息中，并以恢复隐藏数据为名向下载者进行小额勒索，至今**已勒索获利4000元人民币**。

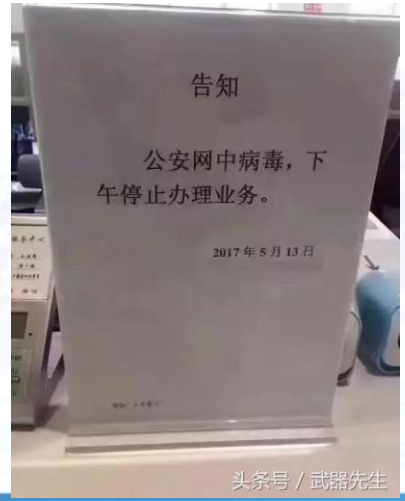
网警提醒

广州市公安局网监分局负责人提醒网民:不要轻易登录不明人员发来的电子邮件或手机短信息中提供的“精彩网址”，这或许就是各类骗子向用户的计算机嵌入木马程序(黑客软件)的阴谋，并以此盗取用户的个人资料或信息。

“WannaCry”等勒索软件“攻城掠地”

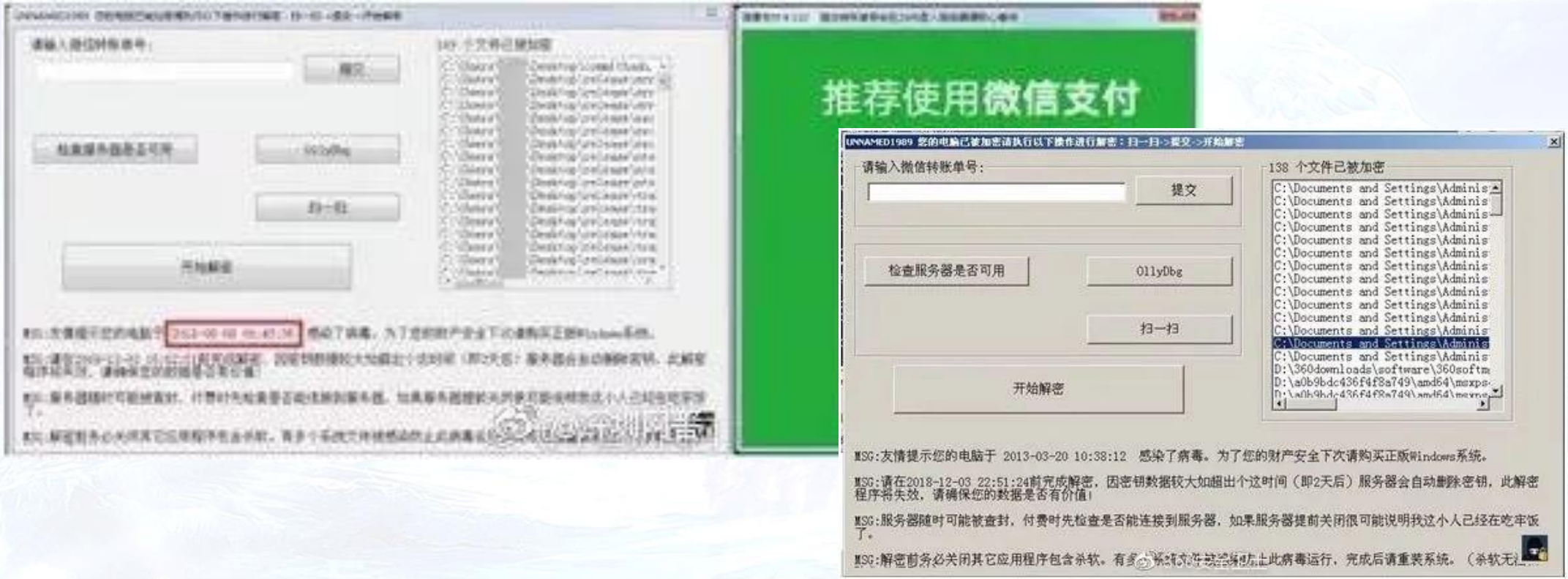


74 countries hit, security firm says



使用微信支付赎金

- 2018年12月1日，国内首次出现了要求微信支付赎金的勒索病毒



网络钓鱼活动猖獗

窃取工行帐号密码的网银木马

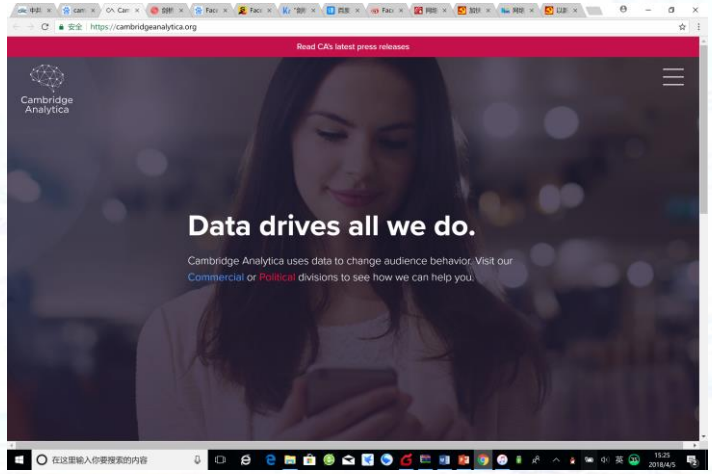
数据泄露事件频发

Facebook数据泄密

剑桥分析公司收到了剑桥大学讲师 Aleksandr Kogan的数据。据称Kogan创建了一个名为“thisisyourdigitallife”的应用程序，该应用程序表面上向用户提供个性预测，并称自己是心理学家的研究工具。

该应用程序要求用户使用他们的Facebook帐户登录。作为登录过程的一部分，它要求访问用户的Facebook个人资料，位置，他们喜欢的服务，重要的是，他们的朋友的数据。

Facebook说，问题在于Kogan在没有用户许可的情况下将这些数据发送到了剑桥 Analytica，这违反了社交网络的规则。“剑桥分析”公司在竞选期间与美国总统特朗普合作，非法获取5000万“脸书”用户的信息。根据收集到的信息，研究人员评估了选民的政治偏好，并直接按照其兴趣向选民投放广告。



新加坡遭史上最严重APT攻击

- 黑客利用被恶意软件感染的计算机，在2018年6月27日和7月4日之间非法访问了新加坡的人口医疗数据。被泄露的数据涉及了150万新加坡人的健康记录，其中包括总理李显龙！这是"史无前例的"。
- 我不知道袭击者希望找到什么也许他们在寻找一些国家的秘密，或者至少是让我难堪的事情，"李在 Facebook 上写道。 "我的药物数据不是我通常会告诉别人的东西，但是没有什么令人担忧的。

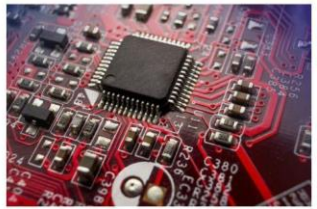
数据泄露事件频发

- 2018年8月28日，华住集团旗下连锁酒店疑似发生用户数据泄露。在暗网，一位ID名为“helen250”的用户发帖出售1.3亿名华住旗下酒店入住用户数据包，泄露数据总数达到5亿条。华住酒店发布的声明称，此信息未经核实，目前集团已经报警，并且聘请技术公司进行核查。
- 8月30日，21世纪经济报道记者联系首先发布信息泄露消息的紫豹科技，他们表示在揭露事实后，遭遇了各方压力，目前不便发表言论。而一位不愿具名的网络安全工程师则透露，目前报道泄露的这些数据已经在暗网中出售，出售人提供了一万条测试数据。
- 据悉，此次被泄露的信息几乎涵盖华住旗下所有酒店，包括汉庭酒店、美爵、禧玥、漫心、诺富特、美居、CitiGo、桔子、全季、星程、宜必思等多个品牌。数据来源包括：华住官网注册资料，酒店入住登记信息以及酒店开房记录三类。信息主要类型为姓名、身份证号、家庭住址、内部ID号以及1.3 亿人身份证等信息。这些数据售价为8个比特币（约5.6万美元）或520门罗币。

四、网络事故频现

一只U盘引发的血案：U盘病毒导致台积电损失超10亿

- 2018年8月3日晚，台积电电脑系统遭到“WannaCry”病毒变种的攻击，造成竹科晶圆12厂、中科晶圆15厂、南科晶圆14厂等主要厂区的机台停线等消息。
- 台积电方面8月5日公告声称，此次事件对2018年第三季度营收影响约为3%，毛利率影响约为1%。8月6日改口称“营收影响将缩小到2%”。此前台积电预计第三季度营收84.5亿~85.5亿美元。也就是说，台积电损失至少在1.69亿~1.71亿美元（约合人民币11.52亿~11.66亿元）。 8月6日，在台湾证券交易所进行的台积电重要信息说明会上，台积电总裁魏哲家亲自出席并反复强调，病毒感染事件为新机安装过程中的“人为操作失误”所致，包括生产资料库、客户资料在内的公司主要电脑系统均不受影响。



阿里云出现故障

2018年6月27号下午，阿里云服务器出现故障，估计很多人都发现自己网站登不进，随后阿里云发布公告称，阿里云工程师正在紧急处理中。下午5点半，部分网站已恢复正常，阿里工程师回复：敬畏每一行代码，敬畏每一份托付。

【异常通告】6月27日阿里云部分产品及账号登录访问异常通告

【阿里云】【异常通告】

异常时间：北京时间2018年6月27日16:21左右。

异常概述：于北京时间2018年6月27日16:21左右开始，阿里云官网的部分管控功能，及MQ、NAS、OSS等产品的部分功能出现访问异常，阿里云工程师正在紧急处理中，请您稍后重试。

给您带来诸多不便实在抱歉！有任何问题，可随时通过服务电话95187联系反馈。

【异常更新】

北京时间2018年6月27日 17:30

目前受影响的产品功能大部分已经恢复正常，请您确认。若还有异常，请您跟我们反馈，谢谢。

北京时间2018年6月27日 16:50

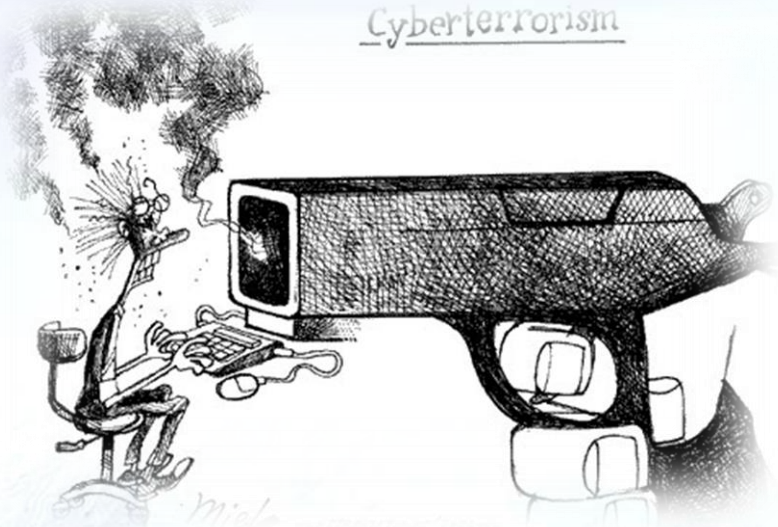
目前受影响的产品功能正在逐步恢复中，若遇到异常，请您稍等后重试。

创业公司投诉腾讯云硬盘故障致数据丢失

- 一家名为前沿数控的创业公司投诉腾讯云，称2018年7月20日，近千万元级的平台数据全部丢失，原因就是选用了腾讯云服务器。前沿数控称，在与腾讯云的交涉过程中他们给出的答复始终是“已向公司相关部门反馈，请耐心等待”。直到事故发生第14天，腾讯云才给出答复，答复是：补偿责任总额不超过腾讯云公司就违约服务收取服务费用总额，另赠一个腾讯云价值10万元的套餐包。前沿数控称，随后，腾讯云很快将赔偿方案中的10万套餐包改为13.29万元现金，说这是他们争取的最大赔偿了。
- “一个创业公司花二年多心血打造的平台就这样被腾讯云给毁了，在公司生与死的抉择关口，腾讯云公司口口声声说重视，他们会对事故负责，我们也期盼腾讯云能提供合理的赔偿资金来还创业公司的一线生机。”前沿数控说，经过苦苦等待十多天，得到的结果却是少得可怜的赔偿。
- 腾讯云发布公告，称希望可以尽快帮助用户恢复业务，将损失降低最低，因此提出“赔偿+补偿”总金额达到136469元的解决方案，这是其在腾讯云平台中用云金额的37倍。“‘前沿数控’基于自身评估就此次故障对腾讯云提出了高达11016000元的索赔要求。”腾讯云说，毫无疑问，这远远高于自身能够提供的方案。这也是此次双方目前未能达成一致的主要原因之一。腾讯云还说，对此次故障给用户业务带来影响再次表示最诚恳的歉意。后续，针对云盘产品会额外实行定期强灾备措施，进一步保障用户数据的可靠性。

五、网络恐怖活动加剧

网络恐怖活动加剧



网络空间已成国际反恐新阵地

1997年，美国加州情报与安全研究所资深研究员柏利·科林首次提出“网络恐怖主义”一词，认为它是“网络与恐怖主义相结合的产物”。同年，美国联邦调查局专家马克·波利特对此进行补充，认为“网络恐怖主义是有预谋，有政治目的，针对信息、计算机系统、计算机程序和数据的攻击活动，是由次国家集团或秘密组织发动的打击非军事目标的暴力活动”。此后，网络恐怖主义的定义不断完善。2009年，联合国“反恐执行工作组”（CTITE）将其界定为四类行为：“第一类是利用互联网通过远程改变计算机系统上的信息或者干扰计算机系统之间的数据通信以实施恐怖袭击；第二类是为恐怖活动目的将互联网作为其信息资源进行使用；第三类是将使用互联网作为散布与恐怖活动目的有关信息的手段；第四类是为支持用于追求或支持恐怖活动目的的联络和组织网络而使用互联网。”

2012年，联合国“毒品和犯罪问题办公室”（UNODC）将其定义为“故意利用计算机网络发动攻击以扰乱如计算机系统、服务器或底层基础设施的正常运行”。伴随恐怖组织熟练运用网络与信息化技术，“网络圣战”“数字圣战”“新媒体恐怖主义”“恐怖主义2.0”等新概念纷至沓来，恐怖组织的网络化发展态势难以阻挡，改变了国际社会对恐怖主义与反恐的传统认知。

尽管国际社会对网络恐怖主义尚未有统一概念，但作为恐怖主义犯罪的表现形式之一，网络恐怖主义的最终目标仍是希望借助网络空间，更为便利、有效地对现实世界制造危害与社会恐慌，壮大恐怖势力。因此，一切以极端主义、暴力和恐怖活动为目的，通过网络实施的相关活动均可列入网络恐怖主义范畴。具体可分为两大类，一是以网络为攻击目标，如针对目标国家政府和关键基础设施的网络入侵行为。二是以网络为战略动员工具，主要包括鼓动宣传、招募培训、筹措资金、勾连策划等，以此作为其实现恐吓与胁迫的手段。

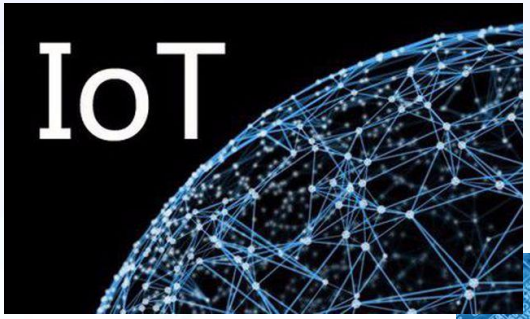
恐怖组织熟练利用网络技术

恐怖组织凭借对网络技术的娴熟运用，极大缓解其当前面临的军事、财政、组织和追捕压力。2015年11月，《连线》杂志披露IS制作的《网络安全行为手册》，详细介绍其网络使用方法：强调优先使用推特并提供12条安全建议；使用加密社交软件，使用加密手机，利用隐蔽性强、难以追踪身份的“暗网”技术，使用服务器位于瑞士的安全电子邮箱服务ProtonMail，使用阅后即焚应用软件等。

为确保战术保密，IS还提供24小时的服务窗口“圣战帮助站”。即使上述工具都被禁止，极端分子仍拥有“圣战者的秘密2”等多种自我研发的软件。这些技术都会将文字转变成混乱的计算机代码，防止安全人员在短时间内破译。2017年伦敦议会大厦恐袭案凶手哈利德·马苏德在袭击前即是使用加密社交软件发送加密信息而未被及时发现。

六、新技术新应用新风险

新技术快速发展


IoT


BIG
DATA
大数据
ADTIME
分析
可视化
实时性计算
长时段跟踪
可视化数据仓库


人工智能


云计算


区块链

新应用不断创新

技术前进一小步，管理升级一大步！

六、政策法律风险

欧盟GDPR《一般数据保护条例》

2016年4月，欧洲议会通过了《一般数据保护条例》(简称“GDPR”)法律条例并将在2018年5月25日生效。 非欧盟成员国的公司(包括免费服务)只要满足下列两个条件之一：

(1)为了向欧盟境内可识别的自然人提供商品和服务而收集、处理他们的信息。

(2)为了监控欧盟境内可识别的自然人的活动而收集、处理他们的信息。

该公司就受到GDPR的管辖。这个条例将对中国企业的移动应用安全，以及数据收集、处理和交易产生重大影响。

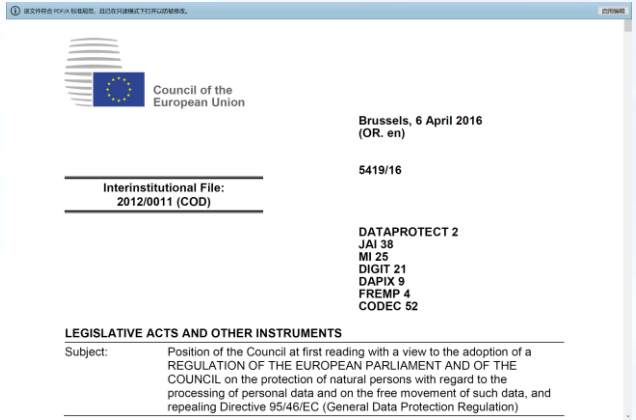
第25条介绍了软件(包括移动应用)开发设计中对数据保护的原则性要求。它强制要求软件在整个开发阶段和运行数据处理阶段能够保护个人数据隐私。

第32条规定了数据控制(含移动应用)和处理需要有足够的技术和措施来确保其数据和移动应用的完整性。这些安全措施必须能够应对数据处理面临的风险，例如所传输或存储的个人数据被篡改、丢失、未经授权披露或被恶意攻击。

以上2条法规是对中国企业移动应用安全合规性的最大挑战。如果没有通过，企业面临的罚款标准是， “一般违规行政罚款的上限是1000万欧元或该企业上一财年全球年度营业总额的2%(以较高者为准)”;“严重违规行政罚款的上限是2000万欧元或该企业上一财年全球年度营业总额的4%(以较高者为准)”。

GDPR规定了欧盟每一个成员国都必须成立关于GDPR的监管机构(“Supervisory Authority”)，负责GDPR在每一个国家的执行。监管机构接受该国关于违法的投诉，有权调查可能的违法情形，并进行相应的处罚。而这一监管机构也有义务和欧盟其他成员国的监管机构沟通，确保在同一件事情上执法尺度尽可能统一。同时，欧盟将设立“一站式”投诉服务，以便于消费者在欧盟内跨境投诉。

对于在欧盟境内有分支机构的中国公司，分支机构将被作为责任主体来强制执行法律要求。 如果没有在欧盟境内设有机构，欧盟将缺席判决，一旦境外公司高管进入欧盟境内，将直接强制执行。中国企业首当其冲的是银行、电子商务、互联网、IT企业和软硬件生产商。



Council of the European Union

Brussels, 6 April 2016
(OR. en)

5419/16

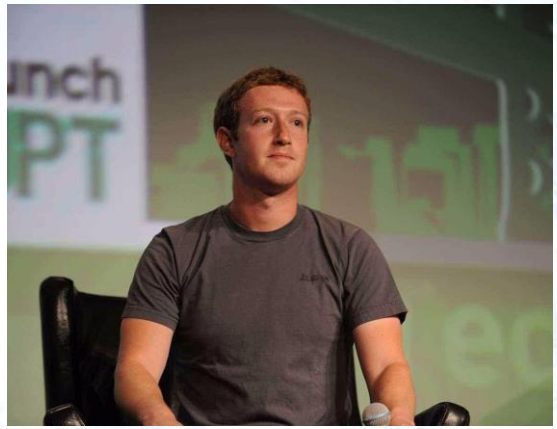
Interinstitutional File:
2012/0011 (COD)

DATAPROTECT 2
JAI 38
MI 25
DIGIT 21
DAPIX 9
FREMP 4
CODEC 52

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Facebook将遵守《一般数据保护条例》



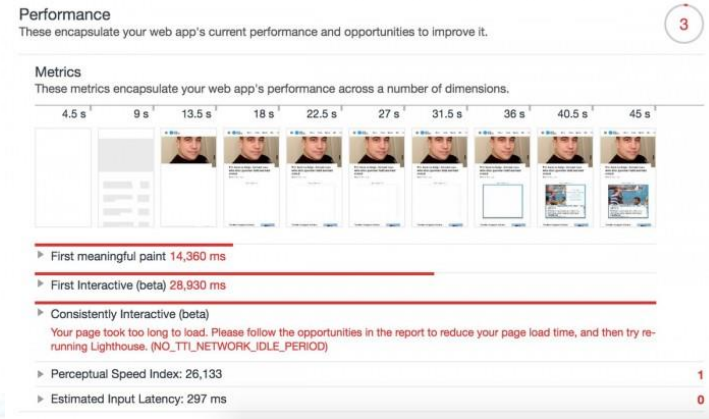
2018年4月4日，马克·扎克伯格与多家重要媒体的记者进行了电话会议，讨论关于 Facebook 如何更好地保护用户数据。当问到GDPR时，扎克伯格回答说：我认为像 GDPR 这样的监管方案是积极的。我对路透社昨天关于 GDPR 的报道感到惊讶，因为记者询问我们是否计划在全世界范围执行 GDPR 的监管，我的回答是 YES。我们打算在全世界各地都执行同样的用户隐私保护标准和功能，不只是在欧洲。全部采用同样的数据格式存档用户数据？也许不是。因为我们需要解决在世界各地符合不同法律要求的方法。

但是，让我重申这一点，我们会保证所有的隐私控制和设置相关功能在世界各地都是一致的，不只是在欧洲。

为遵守GDPR 美国网站屏蔽五亿欧洲居民

欧洲数据保护法 GDPR 于 5 月 25 日生效，众多美国网站纷纷选择站在广告商这边，拒绝了来自欧洲的访客。欧洲有五亿居民，是美国人口的 1.5 倍。拒绝或暂时拒绝欧洲访客的知名网站包括 The Los Angeles Times、Chicago Tribune、The New York Daily News 和 Instapaper。

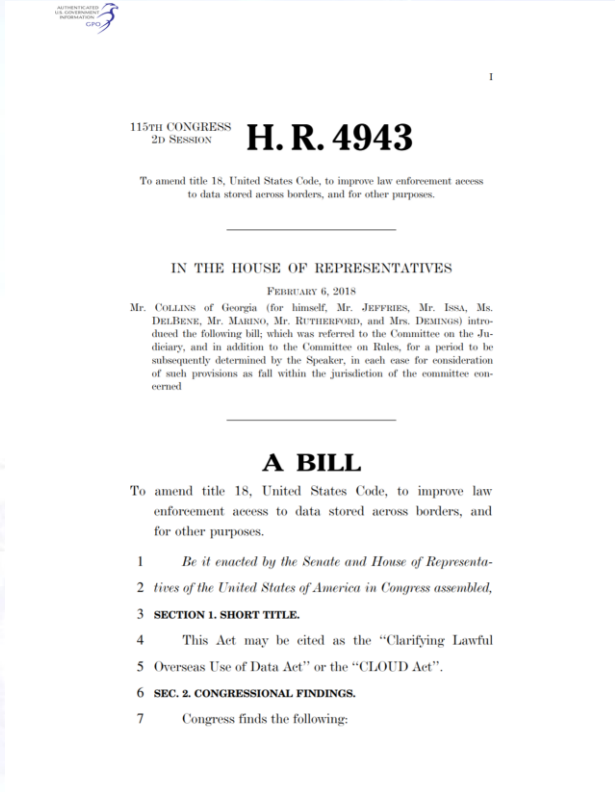
USA Today 则选择为欧洲访客专门制作了一个 GDPR 版本，移除了所有跟踪脚本和广告，**结果美国版本的大小有 5.2MB，而 GDPR 版本只有 500KB**，页面加载速度也从 45 秒减少到 3 秒，JS 脚本数量从 124 个减少到 0 个，请求的网址数量也从超过 500 减少到 34 个，简直就像是最初启用了 ad blocker 的效果。



美国CLOUD法案允许政府跨境调取数据

2018年2月6日，美国参议院和众议院同时提出“Clarifying Lawful Overseas Use of Data Act” or the “CLOUD Act”，也称为“云幕”法案（“S.2383-CLOUD Act”和“H.R.4943-CLOUD Act”），2018年3月22日，众议院将“云幕”法案（S.2383-CLOUD Act）加入到美国政府“2018年（财政）综合拨款案”中并获得通过，2018年3月23日，参议院通过该法案，同日，经美国总统唐纳德·特朗普签署，该法案生效。

CLOUD法案的出台起因于微软与美国执法部门之间的法庭斗争：联邦调查局前往纽约向法院提出索要微软某客户数据的诉求，但该数据存储在微软爱尔兰的服务器上，微软希望检察官前往爱尔兰并经爱尔兰法院许可才能拿到该数据。



115TH CONGRESS
2D SESSION

H. R. 4943

To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 6, 2018

Mr. COLLINS of Georgia (for himself, Mr. JEFFRIES, Mr. ISSA, Ms. DELBENE, Mr. MARINO, Mr. RUTHERFORD, and Mrs. DEMINGS) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Rules, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Clarifying Lawful Overseas Use of Data Act” or the “CLOUD Act”.

SEC. 2. CONGRESSIONAL FINDINGS.

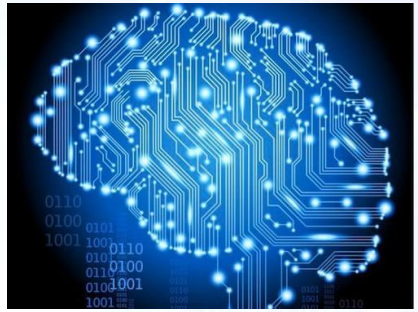
Congress finds the following:

长臂管理趋势

网络空间面临的主要风险

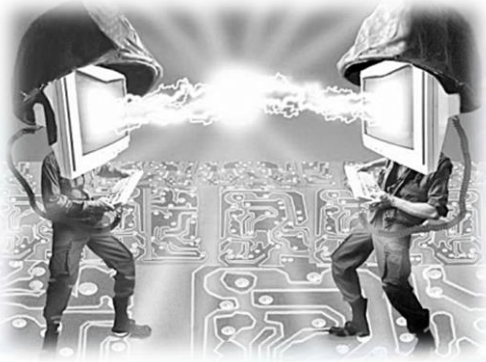
网络犯罪

网络事故



技术风险

网络恐怖



网络战争

政策法律

02 网络安全态势感知研判工作

协会组织态势感知研判工作的背景

2017年6月1日《网络安全法》正式实施，其中指出：国家建立网络安全监测预警和信息通报制度，国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

国务院《“十三五”国家信息化规划》中指出：全天候全方位感知网络安全态势。加强网络安全态势感知、监测预警和应急处置能力建设。建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。建立政府和企业网络安全信息共享机制，加强网络安全大数据挖掘分析，更好感知网络安全态势，做好风险防范工作。

习近平总书记在主持召开的网络安全和信息化工作座谈会时提出，“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”

中央网信办作为统筹协调国家网络安全保障体系和可信任体系建设，牵头协调有关部门制定相关行业网络安全规划及保障评价指标体系，协调国家网络安全整体工作的重要部门，在构建国家网络安全保障体系过程中，需要掌握全国的网络安全态势及重点行业、关键信息基础设施等受到或可能遭受的网络威胁攻击情况，从而为决策指挥提供依据。

中国网络空间安全协会作为中央网信办指导下的网络安全领域的全国性社会团体，旨在发挥桥梁纽带作用，组织和动员社会各方面力量参与中国网络空间安全建设，为国家提供网络安全领域战略服务，促进中国网络空间的安全和发展。我会将全力配合网信办工作，从行业角度出发，协调各方资源为我国网络安全整体态势感知情况提供专业支撑力量。

主要工作

1. 定期组织召开国内网络安全企业、专业机构分析研判当前网络安全形势和下一阶段面临的网络安全态势情况。
2.与国外主要网络安全企业建立沟通联系机制，共同发现、用对全球行大规模网络安全突发事件，做好网络安全应急响应工作。
3.通过对过我网络按期按行业日机构的调研，掌握一线网络安全态势感知技术，了解下一步态势感知线技术，新应用情况。

充分发挥行业协会的组织动员能力，协调各方面力量建立网络安全信息定期通报机制，发现重大网络安全风险和威胁第一时间研判，对今后可能存在的网络安全隐患及时向网安局汇报。

工作情况

A

初创网络安全态势行业会商机制

B

成立网络安全态势研判工作组

C

定期召开网络安全态势专题研讨会

D

定期提交网络安全态势报告

建立行业会商机制

网络安全态势行业会商机制：

2018年7月，协会组织网络安全态势感知专题研讨会，会上研究确定建立网络安全态势研判行业会商机制，该机制得到了主管部门的高度肯定。

成立研判工作组

研判工作组
成员单位
（11家）

北京邮电大学

安天、 360、阿里、安恒、恒安嘉新

美亚柏科、锐安科技、
任子行、深信服、网宿科技

定期召开专题研判会

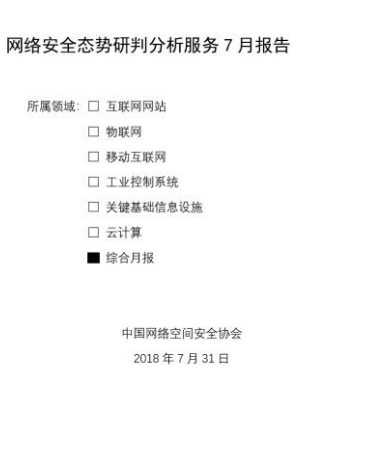

研判会（8次）
7月态势研判
8月态势研讨会（9月6日）
9月态势研判会（9月28日）
10月态势研判会（10月30日）
11月态势研判会（11月22日）
12月态势研判会（12月27日）
年度总结会（1月中旬）
7月态势研讨会（8月22日）
7月报告评审会（7月30日）

领导专家重视支持

编制报告

报告（10份）

1. 月度报告6份（7月-12月）
2. 调研报告2份
3. 年度报告1份
4. 工作报告1份



网络安全态势研判分析服务 7 月报告

所属领域：☐ 互联网网站
☐ 物联网
☐ 移动互联网
☐ 工业控制系统
☐ 关键基础信息设施
☐ 云计算
■ 综合月报

中国网络空间安全协会
2018 年 7 月 31 日

网络安全态势研判分析 12 月报告

所属领域：☐互联网网站
☐物联网
☐移动互联网
☐工业控制系统
☐关键信息基础设施
☐云计算
☐安全情报
■综合月报

中国网络空间安全协会
2018 年 12 月 20 日

网络安全态势研判分析 2018 下半年度
综合报告

所属领域：☐互联网网站
☐物联网
☐移动互联网
☐工业控制系统
☐关键信息基础设施
☐云计算
☐安全情报
■综合报告

中国网络空间安全协会
2018 年 12 月 20 日

03 态势感知工作的一些思考

什么是“态势”

态：状态。快照，静态的?
势：形势。发展趋势，动态的?

重温习近平总书记4.19讲话

全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。

维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。感知网络安全态势是最基本最基础的工作。要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。

有专家反映，在数据开放、信息共享方面存在着部门利益、行业利益、本位思想。这方面，要加强论证，该统的可以统起来，发挥1+1大于2的效应，以综合运用各方面掌握的数据资源，加强大数据挖掘分析，更好感知网络安全态势，做好风险防范。这项工作做好了，对国家、对社会、对企业、对民众都是有好处的。

态势感知工作要点

1.目标要求：全天候全方位感知网络安全态势。知己知彼。感知网络安全态势是最基本最基础的工作。 （两全两知两基本）

2.方法步骤：要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。（态势感知六步法）

3.机制保障：网络安全风险报告机制、情报共享机制、研判处置机制、信息共享机制。龙头企业要带头参加这个机制。（四项保障机制）

以两全两知两基本为目标，以六步工作法为手段，以四项机制为保障，提高网络安全防控能力。

成果与问题

A

成果：

1、初创网络安全态势行业会商机制。

2、成立网络安全态势研判工作组。

3、超额完成合同规定报告数量。

4、充分发挥协会桥梁纽带作用，为政府部门提供有力支撑。

成果与问题（续）

B

问题：

1、缺乏网络安全态势相应标准。

2、缺乏与国外相应网络安全信息机构的交流合作。

3、研判的时效性和前瞻性还需提升。

4、数据类型和范围还需扩充。

下一步工作安排

A

牵头组织起草网络安全态势感知相关标准。

B

深化完善网络安全态势行业会商机制。

C

拓展国内外网络安全信息渠道，全面掌握网络安全态势。

D

推动网络安全态势感知平台建设。

谢谢!

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰