斯诺登效应的前因解读
——Cyber空间相关的博弈思考

肖新光
安天实验室
特邀专栏作家

关键词：斯诺登　棱镜　隐私　情报　网络空间战

事件要点

2013年6月，前美国中央情报局雇员、现国家安全局防务承包商博斯艾伦公司(Booz Allen Hamilton Consulting Firm) 雇员爱德华·约瑟夫·斯诺登(Edward Joseph Snowden) 揭露了美国政府的相关秘密监控工程和入侵行为[1]，导致全球舆论震荡，被媒体称为“棱镜门”。在此过程中，“棱镜”虽然是一个高频上镜的语汇，但并不足以代表相关信息的全部内涵。

我们把斯诺登所披露的信息和近期媒体报道的其他关联信息进行了汇总，如图1 所示。

其中值得特别关注的信息包括：1“ 棱镜”工程是美国国家安全局(NSA) 所使用的网络情报系统的一个组成部分，主要任务是利用美国主要互联网企业所提供的接口进行数据检索、查询和收集工作[2][3]。2 从目前的信息看，谷歌、微软、苹果、脸谱等美国主流IT 企业大多与此计划有关联[2][3]。3 美国国家安全局下属机构TAO，对中国进行了长达15 年的攻击，相关行动得到了思科的帮助[4]。

相关事件并非简单的监控与隐私泄露问题，其影响纵深涉及到当前全球秩序、外交、情报与内政的诸多方面。

大格局表面上的平静能被小人物轻易打破，往往说明旧有的平静乃是假象，平静的背后可能隐藏着不平衡、不平等和被人为制造出来的冲突。因此笔者选择了信息失衡、网络空间的情报和交战规则、合法监听权和民权博弈的三个维度，对相关背景进行分析。

从技术失衡到信息失衡

“棱镜”事件之所以会转化为外交问题，其重要原因是**全球信息流向长期不平衡。**一方面，**基于美国IT企业所提供的先进、方便的互联网服务，全球用户个人信息都向美国单方聚合；**另一方面，依托文化、价值观方面持续打造出的优势地位和输出能力，美国持续而主动地对全球的政治与文化进行着深刻影响。

这种局面的形成，是美国**把握重大历史机遇获取了先发优势，并持续执行高质量战略顶层设计将优势扩大的结果，**有历史和地缘的综合因素。但如果我们分析美国走向单极的过程，并将传统欧洲列强信奉的“守夜人”理论[5]与杜鲁门关于三个自由（信仰、言论、企业）的论述[6]进行比较，就会发现其不尽相同，后者对“国家”的理解更加立体——**以军事硬威慑和价值观制高点的软实力作为复合手段，既可达成政治诉求，亦能在经济上扩张并推动本国主流企业摘得更大的全球扩张果实。而美国企业发展、形成垄断的过程，又为美国的国家安全和全球威慑力提供了强有力的支撑。我们可以称之为“带剑重商主义 2.0”。**

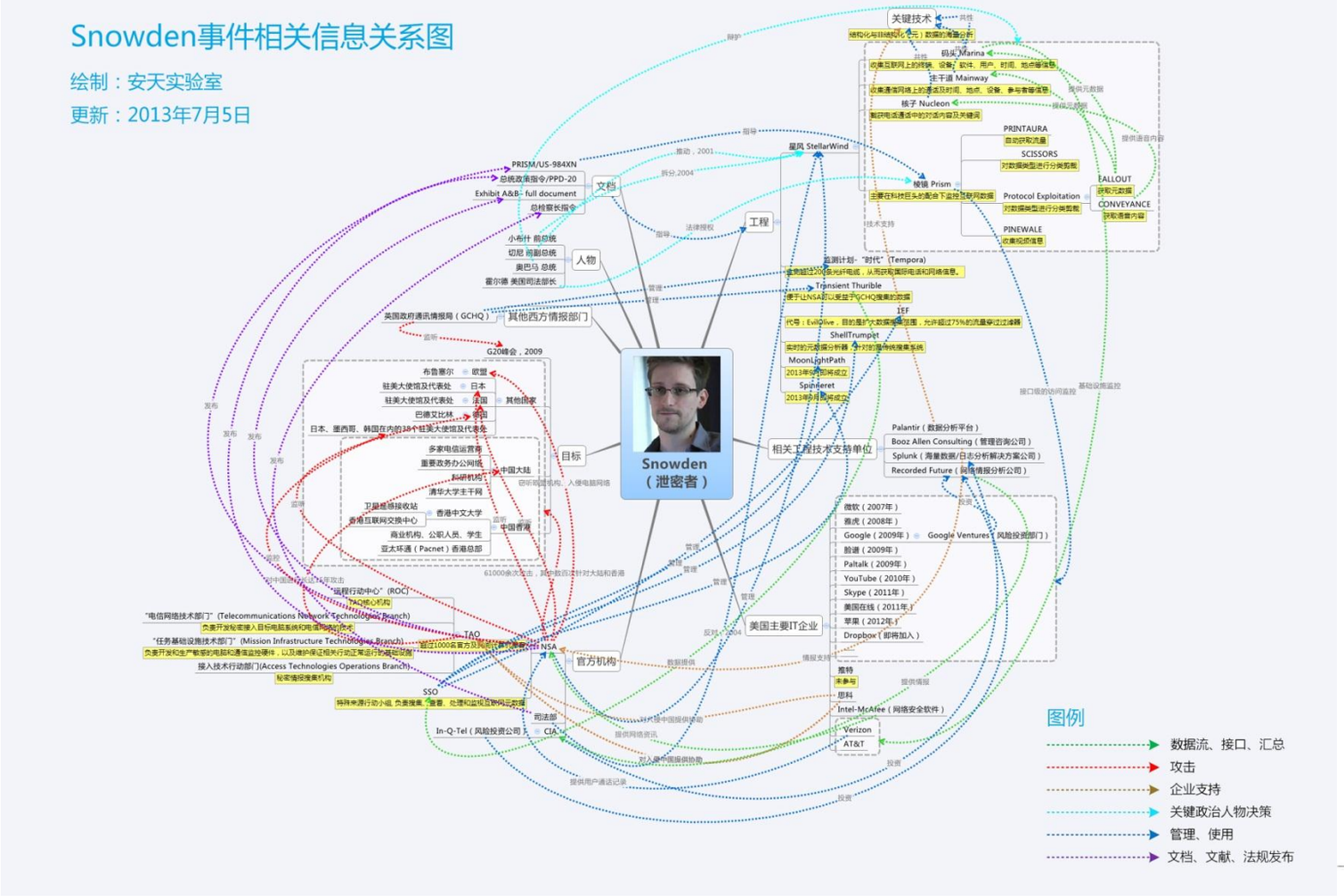

图 1 斯诺登事件相关信息关系图

美国IT 企业对其国家战略威慑力的推动，可以划分成两个阶段。

第一阶段：以技术和产品的优势为主导的时代 其主角是IBM、苹果（PC 时代）、微软、英特尔、思科、甲骨文等高科技软硬件产品企业。伴随着PC 革命的启动，美国**在全球IT 供应链中，逐步扮演了大部分关键产品和关键技术的供应商角色，**这一角色被20 世纪90 年代的信息高速公路建设所强化。微软Windows 操作系统、英特尔 CPU 和思科交换路由产品等为代表的美国IT 产品，基本统领了全球信息化进程。

这种对美国IT 产品的重度依赖，亦导致了其他国家严重的“预留”后门恐慌和猜测，部分代表性的事件见表1。

这些传言多数带有阴谋论色彩，缺乏实证支撑。但其中部

表 1 美国软硬件产品的部分后门传言

时间	事件	后续情况和验证结果
1999.8	微软预留美国国家安全局密钥事件[8][9]	微软澄清不具备足够说服力，后来在给中国的源码托管中不包含该部分。
2007.5	赛门铁克查杀微软系统文件致蓝屏，引发微软后门传言[10]	从技术上可以证实此事与微软是否存在后门无关联。
2008.10	微软黑屏事件[11]	本身不具备后门性质，但提出了互联网场景下产品因在线验证和升级导致的新安全问题。
——	英特尔CPU特定指令序列可致自毁传言	为小规模传言，无资料可查，也一直未得到有效验证。
2005.7	思科预留后门传言[12]	传闻中国骨干网某次大面积故障与此相关，但未有分析实证。
2003	FreeBSD 预留后门传言[13]	据说为其作者言论，但仅存孤证，未见有相关验证工作。

分传言的真伪，实际上受第三方分析能力等因素的限制，未得到真正的深入分析和验证，而对应厂商亦未提供有效的证据证实自身清白。随着互联网时代的到来，IT 产品广泛引入了补丁分发、模块和功能推送、Flash 固件升级、远程维护(over the air, OTA）和运维监控等级机制，此时包括二进制分析、沙箱等诸多传统安全分析手段，以及代码国家托管在内的策略，几乎完全失去了意义。

在第一阶段，美国集成电路与硬件的能力优势、软件基础环境以及配套的知识产权体系等，充分形成了优势高墙。“知识产权问题”则成为巩固相关优势经常使用的武器，如思科对华为的诉讼[7]。这个阶段的积累为美国产业的第二阶段提供了理想的基础和铺垫。

第二阶段：以模式和资源为主导的时代 以谷歌、亚马逊、脸谱、推特等为代表的美国互联网企业，也包括转型后的苹果和微软，开始引领全球生活方式的变革。**基于广泛的信息采集和聚合的思想，互联网企业对海量用户的社会关系、个性习惯、喜好关注、行动轨迹等进行了充分的聚合、分析和挖掘，并对用户体验给予了前所未有的高度尊重，其优质服务和体验与普遍的免费方式相结合，开始改变全球网络用户的生活模式。**

计算和系统是信息生产的工具和载体，但并不是信息本身，第一阶段的基础设施的先发优势为第二阶段的信息聚合能力提供了基础保障。这一模式带来的重大信息流向变局是：**全球用户以放弃部分隐私为代价来置换高质量的免费信息服务，主动向云端提交个人信息[14]。**

但如果把这种模式引入安全考量的话，这种模式究竟有怎样的威慑力，以无线安全试举一例：

从安卓 4.0 版本开始，谷歌内置了Wi-Fi 密码远程备份的功能，而且默认开启。这个功能给用户带来的方便不言而喻，当用户购置了新手机后，只要重新登录自己的谷歌账户，就可以取回全部连接过的无线接入点的密码，而不用逐一重设。但如果换一个角度来看，由于谷歌通过该功能获取了无线接入点的服务集标识符(service set identifier, SSID) 与口令信息，同时安卓系统采用了Wi-Fi 信号辅助进行定位，因此意味着谷歌通过定位、地图服务的广泛应用和采集，掌握了大量无线接入点的位置信息；再辅以谷歌遍布全球的街景车，**使谷歌具备了监听全球Wi-Fi 网络的能力（当然能力的具备并不代表有相应的意图或者行为）。这种能力是模式颠覆的结果，其让任何基于传统分布式集群和图形处理器加速的破解体系无论何其庞大都无法望其项背[14]**。而这个能力却只是整个体系能力非常微小的一部分。

谷歌一直以“不作恶”的企业原则，来抵消外界对其企业能力的质疑。但如果谷歌将相关数据向美国情报系统开放的话，那么这些信息的直接攻防价值就不言而喻。

国家战略优势一旦形成，将给优势方带来持续的国家红利回报，同时也会带来失衡方的恐慌与反制。但我们看到的多数反制手段都是基于对反垄断规则的采用，例如几年前欧盟对微软的捆绑、预装等行为的多次诉讼[15][16]。实际上，在个人电脑操作系统层面，欧盟产业界并无与微软分庭抗礼的可能性，因此这种垄断诉讼基本都是对美国企业内战（如网景起诉微软）的低级模仿，只能从浏览器、播放器等外围环节入手，欧洲本土的IT 企业亦未能从这些诉讼中真正获益或崛起。

在第二阶段，美国的**优势从技术优势变成模式优势，甚至被当作价值观的高点，这种优势几乎无法破袭，**包括欧盟国家提出收取“流量费”的思路[17]，都显得无奈而稚嫩。而谷歌街景车抓取Wi-Fi 数据一事，先后遭到了多国政府的调查[18]，但基本都是跟进媒体舆论做出的被动反应，最终多半以“吃大户”、“敲竹杠”式的罚款了事，“板子”高高举起，轻轻落下。

而美国在确立了明确的战略优势后，及时通过了爱国者法案[19]，确立了对IT 寡头们进行管理的法律依据，从而**实现了其依托其国内法律授权就可以监控全球互联网的空前优势。**这种优势是一种难以动摇的既定事实，即使因偶然事件为导火索，引发出劣势方无奈且效果有限的反弹，也会因底气不足和优势方的拆招化解，而消于无形。

网络交战原则和情报获取原则的大国博弈

斯诺登所披露出的美国对包括中国在内的多国互联网目标进行攻击的信息削弱了美国一直营造的语境氛围：即通过“APT1”等报告[20]和配套的舆论攻势，将中国打造成全球互联网安全的公敌，而把自己塑造成受害者+ 正义者的形象，美方这个战略一直大获成功，而这个语境中也包含着美国综合的诉求。

如果从这些诉求中拨开舆论战的浮云，也剥离其背后具有美国军方向国会申请增加网军预算的公关色彩，而去关注较长一段时间以来美国院府和情报机构人士的观点表达，则同样可以看到其期望利用营造出的舆论主动：**在大国确立网络交战和网络情报获取的原则的过程中，占领谈判制高点，获得规则制定的主动权 。**

下面的言论在一定程度上代表了美国在制定相关原则上的核心诉求：

● 美国政府也对其它国家进行网络间谍活动，但最大的区别是美国政府不会以入侵欧洲空中客车的方式将空客的秘密告诉波音公司。——前白宫安全顾问理查德·克拉克(Richard Clarke)[21]

● 因为无法向中国上空派遣无人机，所以我们需要向中国派出间谍。——美国中央情报局高级官员洛文塔尔(Lowenthal)[22]

● 为了保护知识产权，美国企业应在产品中嵌入病毒。——美国参议员奥林·哈奇(Orrin Hatch) 等[23][24]

● 如果你关掉我们的电网，我们就冲你的烟管扔导弹。——五角大楼某官员[25]

为了探究这些规则诉求的原因和背景，我们将中美相关领域现状进行对比形成表 2。

表 2 中美相关领域现状对比

	美 国	中 国
传统情报获取手段和能力	绝对领先	落后
军事发展水平	全球绝对领先	普遍落后美国10年以上，有的甚至多达 30~40 年
网军	全球最庞大规模网军	不详
关键行业和部门的保密思路	依托有效的防护手段和IT 治理策略与能力	主要依赖物理隔离
IT 基础设施	核心技术和关键产品完全有自身制造	对美国有严重依赖

从传统情报手段来看，美国凭借侦查卫星、无人机、远程预警雷达和预警机、高空高速侦察机、电子侦察船、地面监听站、声纳浮标等形成的覆盖全球的“梯队”[26]和其他电子侦查体系，无论从技术先进性还是从部署能力和范围上，都不存在被其他国家超越的可能性。因此，**美方并不惧怕传统情报领域的挑战，同时也希望获得在网络这一新的情报获取原则上的规则主导权。**

从信息化建设和IT 体系弱点上看，美国有着信息技术的优势，更多着眼点在于从网络互联和信息分享中获得发展动力。据报道，美国的国防、军工等企业依托其强大的IT 管理和安全能力作为保障，与互联网保持联接，其工业体系也广泛接入和利用互联网。因此**美国IT 体系确实存在潜在受攻击面(attack surface) 更宽的情况。**这是美国的核心焦虑点之一，这也正是自2010 年以来美国国家标准技术研究所(NIST)、云安全联盟(CSA) 等机构多次在不同场合强调供应链安全的重要性之所在。而中国严重的焦虑感则来自**基础信息环境对美国信息技术的深度依赖，**这是巨大的信息战劣势。加之中国IT 治理能力和人员素质较低，决策者思路亦较为保守，所以最终在敏感网络和单位广泛地推广了**物理隔离**制度，这种制度尽管给工作和信息交换带来了诸多不便，长期被诟病为鸵鸟政策，但确实降低了国外通过公共互联网进行入侵和渗透的可能性。因此如果我们把美方关于“因为无法向中国上空派遣无人机，所以我们需要向中国派出间谍”的表达，与本次“棱镜”事件连锁曝光出的美国试图潜入中航工业成都飞机工业（集团）获取歼20 资料的信息联系起来看[27]，把这句话替换成

“因为无法通过网络获取到更多的我们想要的情报，所以我们需要向中国派出间谍”，其实也同样成立。

把美国相关的言论转化为原则诉求和与背景原因的对应关系，可以形成表 3。

表 3 美国情报原则诉求与原因分析

美方希望建立的情报作业原则诉求	原因分析
保持传统情报领域的相关格局与潜规则不变	美国具有传统的压倒性优势领域，美国并不担心任何挑战
通过网络攻击获取情报应该是合理的情报渠道	美国网军和情报系统具有强点能力，美方希望强化
通过网络获取的情报不应用于推动本国企业发展	美国是领先者，并不需要过多依赖情报助动
美国的全球基础信息环境的供应优势，应该可以在国家安全和情报作业中使用	这是美国具有压倒性优势的领域，已经以此为借口完成了对中国华为和中兴等企业的打压

但经过信息检索，笔者发现：美国自身并不遵守“情报作业不应用于推动本国企业发展”。2001 年，空中客车公司向欧盟状告波音公司借助美国国家安全局的“梯队”系统获取商业利益，并形成对应调查报告[28]。调查结论为：“National Security Agency, through an electronic surveillance system called Echelon, routinely tracks telephone, fax, and e-mail transmissions from around the world and passes on useful corporate intelligence to American companies.”（美国国家安全局，通过使用被称为“梯队”的电子监控系统，定期跟踪电话、传真和来自世界各地的电子邮件传输，并把对企业有用的情报提供给美国公司）。

从这一点来看，美国相关表达的着眼点其实更为聚焦，更多的是**不希望他国通过情报获取美国军事技术后，直接进行模仿。**仅就中美两国军事工业能力而言，中国的多数基础武器装备普遍落后美国10 年以上，有的多达30 至50 年，美国尽管有试探中国实际能力的诉求，但基本无学习借鉴之必要。因此，其焦虑点在于中国武器装备是否会模仿成长，实现快速跨越。

这就会进入另外一个问题，国防与安全是一个游离于社会问题和民用市场竞争之外的特殊领域，**在国家解决自身安全挑战、提升国家安全价值这一使命面前，传统的知识产权等常态社会准则，其实缺乏实际约束力。**国家间的情报攻防行为也与国家政治体制无关，就像以色列和法国虽然同属西方阵营，也有着同样的议会政治制度，但是，以色列依然通过间谍手段，获取到了法国幻影V 战机重以吨计的完整图纸，并仿制出幼狮战斗机[29]。

近期俄罗斯曝光了一名美国间谍，而美国指责俄罗斯曝光间谍的姓名和相貌是一种违反“惯例”的行为[30]。这个案例说明了**大国情报之间的博弈，实际上是一个以非阳光规则和以潜规则为主导的领域，并不在现有的国际法体系和原则的“事实约束”之内。其原则存在于情报获取中产生摩擦的大国之间，是在彼此长期攻防对抗中摩擦并磋商确立的。**

“棱镜”事件曝光的另一重要信息与信息战相关，由《卫报》网站刊发的总统政策指令(Presidential Policy Directive)[PPD-20]中的部分文字为：“This Presidential Policy Directive (PPD) supersedes National Security Presidential Directive of July 7, 2004. This directive complements, but does not affect, NSPD-54/Homeland Security Presidential Directive on ‘ Cybersecurity Policy’ of January 8, 2008; National Security Directive on ‘ National Policy for the Security of National Security Telecommunications and Information Systems’ of July 5, 1990; and PPD-8 on ‘ National Preparedness’ of March 30, 2011.”[31]（该总统政策指令取代2004 年7 月7 日发布的国家安全总统指令(NSPD)-38。该指令补充但不影响NSPD-54/2008 年1 月8日发布的关于“网络安全策略”的国土安全总统指令(HSPD)-23、1990 年7 月5 日发布的关于“国家安全通信与信息系统”的国家安全指令(NSD)-42 以及2011年3月30日发布的关于“国家准备”的PPD-8。）

这些信息，充分显示了**美国在网络空间战争(cyberwar) 方面所做出的系统的、长期的研究和原则准备。**而对于“你关我的

电网，我就向你扔导弹”的言论，则可以看成对网络交战规则的一种表述——即对于攻击工业和民用基础设施的行为，可以遭到美国的反制军事打击，其表明**美国的网络防御与反制能力都是以其传统的武力优势为保证的。**但有趣的是，美国是使用震网(Stuxnet)蠕虫攻击技术攻击伊朗重化工设施（铀离心机）的重要嫌疑人（另一个是以色列）[32]。其实这种表述，一方面反映出美方对于信息化弱点的担心，另一方面，也是依托其军事威慑能力，对伊朗可能的反击做出的潜在警告。

从历史经验看，**优势地位国家，把其在原有领域的已经长期享有的巨大利益，固化为不可清算的既定事实，但同时又把新兴领域孤立开来，占领价值高点，谋求建立对其有利的新规则的方法，实际上是一种语境陷阱。**

通过上述关于情报和网络交战问题的复盘，我们发现这个语境陷阱的设计是：把相关问题与其传统的情报优势脱钩，而与国家道义、知识产权等联系在一起，加之以军事硬实力的威慑，形成高点和筹码。这样既可以**在网络情报作业和交战原则的谈判中，获得更大主动，又不需要在既有的优势领域（传统的情报和军事能力）做出让步。**

政府合法监听权与民权的博弈

从民间舆论来看，“棱镜”事件令人更为关注的问题，是政府合法监听权与民权的博弈。

奥巴马声称“棱镜”项目不针对美国公民，从目前披露的信息文档来看，有文档可以作为辅证。但事实上，其进行国内监控的还有其发展自“Omnivore”的相关传统机制[33][34]。**“棱镜”项目是否监控美国公民和美国政府机构是否监听美国公民其实并不是一回事。**

笔者希望指出的是：尽管人们大多有生活在不被监听的世界里的愿望，但**合法监听权，是现代政府最为重要的公共安全手段之一，是国家基础支点之一。只要政府承担公共安全职能，就必然需要拥有公共安全手段。**

公共安全手段的价值不言而喻，既包括对公民生命和公私财产侵害的追缉能力，也包括对正在发生的侵害和产生连锁后果的响应能力；同时也会提升酝酿中的和潜在危害的实施成本，增加心理威慑力。在此问题上，无政府主义者和类似电子前哨基金会(EFF) 等一些非政府组织的观点，尽管足够前卫和富有理想主义，但这对任何一个大国来说，都不具备可行性。

公民不论从情感意愿上是否接受政府拥有公共安全手段，亦都享受了公共安全服务。当然政府也必须意识到，**监听权具有双刃剑色彩，越是有效的手段，就越可能对民权造成重度的侵害。**因此，不在于政府是否具备了监听手段，是否实施了监听行为，而在于用于规范和约束监听的法律框架是否存在、条文是否合理，以及是否得到了遵守。

对于合法监听权，个人认为需要符合下列特点：

授权性 监听的方式、手段、对象选取的原则等需要经过法律授权。

特定性 监听要针对明确的目标，或者基于一定的线索触发，不应是无节制和无条件的。

备案性 监听行为应该是有留存记录的，具备可审查和可追溯的特点。

传统的公共安全，由于存在空间边界，界定比较简单，通常以个人居所作为私密领地（只有获得非常明确的证据和法律和授权，才可以实施监视、搜查等），而以公共道路、邮政、电报、电话等，作为可实施合法监控的领域。这一点与早期以个人电脑为端点的网络类似，将传统个人电脑终端视为个人私密领地，将网络通讯视为可以实施合法监控和管理的领域。

在云时代，用户的私密信息开始从存储于终端变为大量聚合于云端，这一方面给用户带来了更好的体验，但另一方面无形中使这些数据逃逸出了用户主机的物理边界，也逃脱出如个人防火墙、本地数据加密等传统的个人终端安全防护手段之外，从而带来了信息在云端失密或者遭遇被滥用的风险。

用户存储于云端的信息，究竟是传统的政府可监控的信道、公共基础设施的组成部分，还是传统的个人私密空间的延拓？这本该是一个被慎重讨论的法律问题。但实际上，在这一法律问题

尚未被明确地广泛讨论和引发公众思考时，“棱镜”等系统就获得了授权。

以iMessage 为代表的消息通讯、以Gmail 为代表的免费邮件等产品，在信道安全能力上的加强，使服务器端几乎成为了唯一可以实施监听的位置。但也需要看到的是，传统通讯监听是根据嫌疑人的位置展开的，是局部而非全局的，即使出现滥用，也是一个局部的事件，而如果要求主流互联网服务商提供相关的访问接口，其威力是巨大的，但如果出现滥用，其对法治的破坏力远大于传统监听手段。

这种手段不仅应该符合政府合法监听权的基本法律约束，而且在体系和流程设计上需要满足**集中、可控、受限**的架构原则，否则即使其法律框架完备，也会导致其被使用者滥用，或者遭到入侵引发数据泄露，演化成民权灾难和其他后果。而从目前所暴露出的消息来看，尽管“棱镜”系统是“星风”计划不能通过司法审查的拆解结果之一，但我们可以从中看出，美国政治结构设计的平衡原则亦在一定程度上得到了体现。而从美国民意反馈来看，有超过半数的人认可通讯监听，这说明在长期生活在反恐的语境条件下，美国民众在这个问题上的态度反而十分理性[35]。“斯诺登事件”或许让全球更多人看到了美国国家机器的能力强大、体系庞杂、背景复杂；这个大到无形的肌体，一直以来都是很多人关注和研究的对象，但还没有到对其做出终极评价的时候。至于美国是否存在着阿罗·拉索(Aaron Russo)[36]所预言的“从自由到法西斯”[37]的倾向，最终只能由历史给出结论。

从地缘政治和大国博弈的角度来看，**拥有战略支配能力的领跑国家，必然会充分利用其先发优势，实现其自身利益最大化。**这种先发优势的利用，也必然伴随着对跟跑者的打压。**这种打压只取决于跟跑者接近的程度和超越的意图，并不取决于追赶的方式。**对于这种严苛的历史规律，过度情绪化的反弹没有任何实际价值。那些仓促的、单维度的结论无论指向何方，只能带给人简单的快感或者痛感，却无法给一个民族的成长以任何教益。

从某种意义上说，“棱镜”事件可能成为中美在相关领域进行缓和并确定新规则的一个契机，也是中国对顶层设计和执行、政府能力与法制建设等多方面进行自我审视和反思的机遇。放弃者永远沉沦，模仿者永远跟跑，自满者可能倒退，唯自省、自新、自强者方有未来的位置。对于那些期望中国成为一个真正的大国，希望国民真正分享到国家红利的人们来说，当看到领跑的冠军国家偶尔踉跄之时，不应拍手叫好，而应加快自己的脚步。■

致谢：感谢我的同事Angel、Billy、Lily、Leaf Gao 等对本文的贡献。

肖新光

网名江海客。CC F高级会员。安天实验室首席技术架构师。主要研发方向为反病毒引擎、大规模恶意事件样本的流水线处理、计算机犯罪取证等。

seak@antiy.com

参考文献

[1] 维基百科：PRISM. http://en.wikipedia.org/wiki/PRISM_(surveillance_program) «

[2] U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html «

[3] NSA taps data from 9 major Net firms. http://www.usatoday.com/story/news/2013/06/06/nsa-surveillance-internet-companies/2398345/ «

[4] Inside the NSA's Ultra-Secret China Hacking Group. http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group?page=0,0 «

[5] [英]亚当·斯密，国民财富的性质和原因的研究(下卷)[M]，王亚南、郭大力译.北京，商务印书馆，1998：252—253. «

[6] Address in New York City at the Opening Session of the United Nations General Assembly.http://trumanlibrary.org/calendar/viewpapers.php?pid=914 «

[7] 《知识经济》：华为诉讼考量中国政府. http://tech.163.com/tm/030307/030307_85353.html «
[8] OpenBSD IPSEC backdoored?. http://lwn.net/Articles/419865/ «
[9] Report of FBI back door rols OpenBSD community. http://news.cnet.com/8301-31921_3-20025767-281.html «
[10] 关于赛门铁克查杀中文 XP 系统文件问题的事件分析. http://www.antiy.com/download/nav.pdf «
[11] Black Screen of Death. http://en.wikipedia.org/wiki/Black_Screen_of_Death «
[12] Cisco backdoor still open. http://www.networkworld.com/community/node/57070 «
[13] FBI 'planted backdoor' in OpenBSD. http://www.theregister.co.uk/2010/12/15/openbsd_backdoor_claim/ «
[14] 安天实验室，肖新光，《互联网用户的泛隐私安全热点问题回顾与浅析》. http://blog.csdn.net/antiy_seak/article/details/8062964 «
[15] Microsoft_litigation . http://en.wikipedia.org/wiki/Microsoft_litigation «
[16] The Commisson's investigation. http://ec.europa.eu/competition/sectors/ICT/microsoft/investigation.html «
[17] Rogers eyes ‘machine to machine’ deals. http://business.financialpost.com/2011/06/17/rogers-eyes-%E2%80%98machine-to-machine%E2%80%99-deals/?__lsa=972f-0d0c «
[18] Google accused of criminal intent over StreetView data. http://www.bbc.co.uk/news/10278068 «
[19] S. 990 (112th): PATRIOT Sunsets Extension Act of 2011. http://www.govtrack.us/congress/bills/112/s990/text «
[20] Mandiant Intelligence Center Report. http://intelreport.mandiant.com/ «
[21] Richard Clarke on Who Was Behind the Stuxnet Attack. http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html?c=y&page=1 «
[22] plan-would-orient-cia-back-toward-spying. http://www.nytimes.com/2013/05/24/us/politics/plan-would-orient-cia-back-toward-spying.html?pagewanted=all&_r=0 «
[23] Dumb Idea Or Dumbest Idea: Letting Companies Use Malware Against Infringers. https://www.techdirt.com/articles/20130527/21352923220/dumb-idea-dumbest-idea-letting-companies-use-malware-against-infringers.shtm «
[24] Senator Endorses Destroying Computers Of Downloaders http://www.techdirt.com/articles/20030617/1445203.shtml «
[25] Cyber Combat: Act of War. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html «
[26] 维基百科：ECHELON. http://en.wikipedia.org/wiki/ECHELON «
[27] Obama will be explained at the G8 summit, “prism”. http://www.stockmarkettodayblog.com/2013/06/17/obama-will-be-explained-at-the-g8-summit-prism.html «
[28] Trade Secrets : Is the U.S.'s most advanced surveillance system feeding economic intelligence to American businesses?. https://www.fas.org/irp/program/process/991101-echelon-mj.htm «
[29] The Israeli Intelligence Services: Deception and Covert Action Operations.Conclusions http://www.historyofwar.org/articles/concepts_israeli_covert.html «
[30] Ryan Fogle: American in ill-fitting wig arrested by Russians accused of being CIA spy. http://www.mirror.co.uk/news/world-news/ryan-fogle-american-ill-fitting-wig-1888718 «
[31] obama-cyber-directive-full-text. http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text «
[32] Iran's nuclear program and a new era of cyber war. http://articles.latimes.com/2011/jan/17/world/la-fg-iran-cyber-war-20110117 «
[33] What was Omnivore? http://curiosity.discovery.com/question/what-was-omnivore «
[34] OVERVIEW OF CARNIVORE. http://carnivore10.tripod.com/id18.htm «
[35] Nearly Half of Americans Want Government to Monitor Everyone's Email, Phone Records. http://www.dailytech.com/Nearly+Half+of+Americans+Want+Government+to+Monitor+Everyones+Email+Phone+Records/article31736.htm «
[36] Aaron Russo . http://en.wikipedia.org/wiki/Aaron_Russo «
[37] America: Freedom to Fascism. http://en.wikipedia.org/wiki/America:_Freedom_to_Fascism «