# 大战略基石——美国信息安全产业格局的解析

安天实验室 / 肖新光

**编者按：孙子兵法云“知己知彼，百战不殆”。在中美网络安全领域“斗而不破”的遏制与反遏制、打压与反打压博弈中，对美方的战略、能力、产业、技术等进行全面综合的了解至关重要。但遗憾的是，过去中方的视角长久的放在关键基础技术领域，放在微软、英特尔、谷歌、苹果等厂商身上，却忽略了美国产业体系中一股强大而独立的力量，其信息安全企业星群，他们也同样是美国全球战略能力的基石。**

在网络信息攻与防的双方向上，美国均拥有着全球最顶级的巨大威慑力和他国看似无法企及的战略优势，而来自中国的观察者易于犯的错误是——既伴着内心深深的忧惧，对这种战略优势进行着轻率地道义层面批判，却缺少对其核心支撑点——信息安全产业的深入而系统地分析。

美国信息安全产业并不是一台生冷而高耸的巨型兵工厂或商业机器，而是一组生动、富有理想与活力的企业符号。长期以来，国内对这些企业符号充满了疑问和不解，一方面，是其传统的巨头 Symantec、McAfee 等始终屹立不倒；另一方面则是新兴企业与新兴技术此起彼伏。巨头型厂商厚重全面的解决方案与独立安全厂商的新概念、新产品交相辉映，令观者应接不暇，更令把美国当作信息化和信息安全建设标尺的各国政府和行业用户茫然无措。

但如果我们把这些企业的规模、并购关系、技术领域、市场范围以及与美国政府的关系，完全罗列开来，进行梳理的时候，就会发现他们并非如突兀坠落在平原上的巨型陨铁，而是有着鲜明的层次和关联的大战略基石。

## 一、美国信息安全产业格局的层次分析

一如美国在其他信息产业领域的优势一样，以 Apple、Google、IBM、Microsoft、Ora–cle、Cisco、Qualcomm、Intel、Facebook（按市值排序）等为代表的基础信息巨头同样在信息安全产业架构中扮演着宽阔而坚实的地基。其稳居全球供应链的顶端位置、进行大量的信息聚合和创造、改变全球用户的工作和生活方式，其一方面构成美国全球战略威慑能力，同时又能反过来游说院府影响美国的政治走向。而透过斯诺登事件，公众们亦知道了，他们与美国的庞大国家机器微妙互动，强化了后者覆盖全球的情报能力。由于这些企业规模庞大、市值往往以千亿美金衡量，并持续进行并购，不断扩容体量，我们可以称其为信息“寡头”企业。

在这些寡头层次之上，则是信息安全产业的巨子们 Symantec、McAfee、Trend micro（趋势），他们市值数十亿美金乃至数百亿美元，尽管这些企业均从反病毒起家，但经过多年发展和持续地兼并重组，其产品跨度已经形成完整的从流量到端的解决方案能力、并向集成、存储、云等安全关联的各方面扩展，产品用户覆盖全球。对中国类似石油、电信、电力等关键行业来说，选择其产品曾长期被视为“政治正确”的选择。

而对更多的安全厂商来说，其依然专注于系统安全、网络安全或其他安全技术的某个窄带领


图1 美国信息安全产业层次结构与主要企业分布

安天实验室制图
2014年4月15日更新
ANTIY

域，可以称其为专业安全厂商或独立安全厂商：

**表 1 一些具有代表性的美国专业安全厂商技术领域分布**

| 技术领域 | 代表厂商 | 备注 |
|---|---|---|
| 网络 | Fireeye | APT 和 0day 防护领导厂商 |
| 网络 | Palo Alto Networks | NG-FW（下一代）防火墙领导厂商 |
| 网络 | Fortinet | UTM 概念领导厂商 |
| 网络 | F5 | WAF 代表厂商之一 |
| 主机系统 | Bit9 | 白名单 + 安全基线方案代表厂商 |
| 主机系统 | Comodo | 传统反病毒厂商 |
| 移动 | Lookout | 新兴移动杀毒厂商 |
| 移动 | Mobileiron | BYOD 安全解决方案代表厂商 |
| 移动 | Zenprise | MDM 代表厂商之一 |
| 移动 | Mocana | BYOD 和移动应用保护厂商 |
| 数据分析 | Solera Network | SOC 的代表厂商 |
| 加密、认证和其他安全领域 | RSA | 加密、认证服务的核心厂商 |

美国专业安全厂商，除了具有单点专注的特点外，大多不仅服务于美国用户，也坚定地追求着全球市场。他们是全球网络安全技术发展的风向标，他们享有“美国制造”的国家品牌带入感，引导着信息安全创新的话语权。但同时他们与寡头和巨头企业不同的是，他们执行更为稳健务实的市场政策，驾轻就熟地寻找当地国家的集成商和掮客企业，通过 OEM 绕过当地政策和法制的保护，如国内很多场合的“国产”防火墙招标就是 Fortinet（飞塔）等美国品牌的“贴牌产品”内战。

随着市场发展，这些独立安全厂商既具有成为新巨头的潜质，同时也有被巨头收购，成为其解决方案中一部分的可能。

而由于美国瞄准全球市场的安全厂商和明星过多，亦掩盖了若干隐形的冠军和一个特殊的市场，即面向其政府和国家机器用户的专用市场。而其中又呈现出两个企业群落，即专用技术企业和承包商。

专用技术领域，是和美国国家机器作业关联密切的技术服务领域，包括入侵取证、数据恢复、数据分析等，这些厂商有的是独立厂商，也有的是巨头厂商或其他大型传统企业（甚至是非 IT 企业）的一部分。大数据分析的明星企业 Palantir 作为美国官方的御用安全企业，是这个产业群体的代表之一。

而承包商则往往是更深入情报作业的直接参与和执行者，类似斯诺登所效力的 Booz Allen Hamilton、信号分析处理厂商 Argon ST、面向 C4I 系统的网络安全服务厂商 Gnostech Inc 等。在这个层次上，我们可以看到美国信息安全思想与其国土安全观和全球战略能力的融合。这些厂商不止服务于专用网络信息系统，也服务于关键工业生产、军事装备等领域。安全思想通过这种服务，深达到更多的关键层次领域，达成虚实结合、网电一体。信息安全概念、意识和方法也同时扩散到社会基础、国土安全和军事体系的全景纵深。

通过图 1 我们可以看出，尽管美国信息安全企业技术领域繁多，投资关系复杂，但这其中几条边界非常清晰。

●基础寡头和独立安全厂商的边界：尽管传统寡头厂商不断兼并独立安全厂商以扩大体量，但我们看到的是其既未导致“独立安全厂商消亡”而构成对自由竞争的伤害；同时也没有改变寡头厂商的原有轨迹——他们依然坚定扮演集成服务提供商或者网络服务提供商的固有角色。如 Google 绝不会因为兼并 Virustotal（多引擎扫描服务提供者）和 Zynamics（安全分析工具软件制造商）而变成一个在安全市场上有所动作的厂商。无论规模大小，美国厂商通常都具有简单清晰的模式与价值观。

●开放市场和专有市场的边界：从某种意义上说，以全球市场为目标的美国独立安全产品厂商专注而窄带，使其不会向与国家机

器的情报体系“过从甚密”的方向游移，从而导致伤害其面向全球用户的信任力。而专有市场的存在，亦既有助于形成美国独有的国家安全作业能力，避免信息外泄，同时，也保证这些厂商不必在全球市场收益和美国官方诉求间徘徊，而可以坚定地如被 Fireeye 收购之前的 Mandiant 一样，在中美大国博弈间，充当非官方的技术喉舌（而即使这种并购发生后，Fireeye 也在努力强调“M 部门”与 Fireeye 本体之前的区别）。从这个意义上说，这个层次不仅是一个商业层次，也构成了大国话语权博弈的立体纵深。

●政府、军方与承包商的角色与关系：围绕军方和情报机构承包商体系是重要的美国商业文明特色，其在具体的情报作业层面，弥补了国家机器本身的人力不足，遏制了大政府倾向，而同时也形成了一个独有的信息层次屏障。尽管出现了斯诺登事件，但我们依然要看到，在充分利用信息的联通和共享，主动国家安全能力提升的思路下，承包商层次其实在很长时间扮演了一个信息和作业中间带的角色。同时也可以看到，这些承包商（包括部分专有市场厂商），往往由前军政界人士发起或者担任高管，其也建立了一种约定俗成的合法利益输送层次（旋转门），形成了一种既同谋共赢、又不伤害美国国家能力的特殊（而且是合法的）政商关系。

这个看似严谨又充满活力的庞大体系，并不是某种计划经济的产物，也不是某届或某几届总统班子马基雅维利式先验设计的结果。而是在其“企业自由”的立国支撑点下，持续遵循内部自由竞争、对外强力输出的产物，可以概括为“顶层设计、自由生长、建立规则、强化优势”。

## 二、领跑者：巨头的形成与价值

美国作为计算机和互联网的本土，在上世纪 80 年代的个人计算机革命中，亦诞生了一批其早期安全企业，这其中就包括了被称为信息安全传统三大的 Symantec、McAfee 和 Trend Micro（尽管 Trend Micro 自诩为治理结构跨美、日和台湾地区的国际厂商，而并不完全是美国厂商，但其根本上还是获益于美国的土壤和产业机会，并也在硅谷信息安全群中扮演重要角色）。

他们的共同特点都是创建于上世纪 80 年代，在反病毒领域获得了产业认同和早期价值最大化，而逐步成为拥有了上万名员工、十亿美金量级的销售额的企业巨人。他们当初在反病毒领域获取第一桶金并不偶然，信息安全市场有两个最重要的最成熟的领域，一个是以反病毒为代表的系统（主机）安全领域，一个是防火墙（安全网关）为代表的网络安全领域。这两类产品都是在与主流威胁对抗中不断改进成型，并逐步具备了共同特点，即经过基本的安装配置部署后，就自行成效，可以不经人工干预而产生效果。而相比之下，类似 IDS、扫描器等对使用者的能力和精力有较大依赖的产品，均未能形成较大市场规模。

病毒的威胁在上世纪 80 年代下半期即快速到来，因此主机安全技术的商业化，要比网络安全技术早了十余年。但 “三大巨头”并非唯一的先行者，上世纪 80 年代末、90 年代初，反病毒企业在全球如雨后春笋般浮现，反病毒核心技术“反病毒引擎”的第一技术平台此时亦并不在美国，反而是由 Kaspersky 和 Dr.Solomon 为代表的欧系厂商占据，与美国厂商呈现争锋之势。在这种对垒中，美国国内市场庞大的内需、资本市场的澎湃活力所带来良好融资能力、以及全球市场的布局辐射，让尚在幼年的“三大”站上了巨人肩膀。他们纷纷较早跃上美国资本市场，并开始了持续的并购之路。使之从单一反病毒厂商发展为综合性的全领域解决方案的厂商。在这个美国企业能力不断强化，欧洲企业一边顽强创新、

一边退守自保的过程中，Dr.Solomon 很快被 McAfee 收购，而 McAfee 则完整获得了其先进引擎能力。而卡巴斯基虽然也稳健发展，成为俄罗斯 IT 的旗帜性企业，同时也成为俄罗斯国家安全的支点企业，但从商业上看，其并未成长为可以在市值（估值）和国际市场覆盖能力上与“三大”比肩的巨头。

传统“三大”与美国情报体系是否有密切的互动？目前尚未有公开资料可以证明。如从公开资料上看，至少没有证据显示他们参与了“棱镜”计划，但棱镜更多是 NSA 与具有内容和关系价值的互联网巨头厂商的合作。而安全厂商自身的资源更多是安全事件、端设备环境和流量行为的信息，显然从这个层面上，作为安全厂商的情报价值是不够的。但传统“三大”对全球行业用户的部署到达能力、端和流量的结合手段、与作为安全厂商进行数据采样提交方面的用户先天容忍度，又有独特的情报优势。如果我们关注《Symantec 互联网安全分析报告》，我们就同样可以看到能够采集这些资源所依托的巨大部署规模，以及这些信息所投射的战略价值。

## 三、专业安全厂商的创新迭代与创新方法

在美国独立信息安全企业的星群中，最富有魅力和研究价值的，是其专业安全厂商的创新迭代。在这个过程中新企业、新技术、新公司、新产品品类不断涌现，而从威胁到产品形态的新概念更迭，也让全球跟跑者们叫苦不迭。

无疑这种概括新威胁、定义新概念、形成新品类式的成熟打法，驱动了多家美国网络安全企业从初创到“各领风骚几年”式的快速迭代成长，但这种成功绝不是源自单纯的概念炒作和商业包装，而是有其值得尊敬的内因与外因。其内因是：对新威胁的敏锐把握，丰富的产品想象力，迅速的单点核心技术突破，并形成新形态品类的能力；其外因则是：对于创新的鼓励和宽容，以及鲜明的专有核心技术价值导向。

在美国安全企业创新迭代案例中，其中最闪亮的轨迹，是网络安全厂商 Netscreen、Fortinet、Paloalto Network 和 Fireeye 依次崛起。而其所提出的产品概念，均创造出了细分市场，也依次在基于流量的安全产品中成为独立品类冠军。我们将这四家厂商的要素，绘制成表 2，由此我们则可以看出，这些企业所形成的产品品类概念，绝非空泛包装，而是应对当时主流威胁的结果。

Netscreen 面对信息高速公路建设引领的带宽快速增长趋势，提出了基于 ASIC 的高速

表 2 美国主流网络安全厂商的创新迭代

| 厂商 | Netscreen | Fortinet | Paloalto Network | Fireeye |
|---|---|---|---|---|
| 创建时间 | 1997.12 | 2000.12 | 2005 | 2004.1.1 |
| 上市时间 | 2001.12.12 | 2009.11.19 | 2012.7.27 | 2013.9.22 |
| 核心概念 | 硬件防火墙 | UTM（统一威胁管理） | NG-FW（下一代防火墙） | Advanced Persistent Threat (APT) Attack & Zero-Day Protection |
| 核心概念提出时间 | 1999.9 | 2004.2 | 2007.6.24 | 2011 |
| 主要产业背景 | 信息高速公路建设，网络带宽迅速增长 | 网络应用蓬勃发展 | 网络客户端、社交网络等新形态，带宽进一步增长 | 国家和政经集团间的相互攻击入侵 |
| 主要应对威胁 | 新的流量压力 | 邮件病毒、垃圾邮件 | SNS 威胁、小众协议、僵尸网络 | APT<br>0Day 漏洞 |
| 核心技术方法 | ASIC 专用芯片 | 流还原检测、与传统文件病毒检测技术结合 | 精细协议解析<br>身份 ID 识别<br>可视化<br>基于多核体制和专有实现的高性能 | 沙箱前置<br>场景组合遍历<br>多向量检测<br>云端能力<br>异步检测与实时防护联动 |

硬件防火墙的思路；Fortinet 面对网络应用发展带来的邮件蠕虫、垃圾邮件、广告软件等威胁，提出了“统一威胁管理”的概念；Paloalto Networks 面对互联网客户端和 SNS 的大发展等带来的新威胁，设计了“下一代防火墙”；而 Fireeye 面对政经集团背景的 APT 攻击大潮，采用沙箱前置与流量产品结合的方法，亦形成了自己独特的反 APT 和 0day 漏洞的产品形态。

这四个厂商的创新过程，都是典型的硅谷路线。强力的技术核心团队迅速得到技术资本的关注和推动支持，在发展的过程中资本给予了研发之路高度的耐心和容忍，如 Paloalto Network 在起步近两年后，产品才基本成型，Fireeye 在成立几年后，才找到了我们今天看到的正确产品思路。更令人称道的是，在他们尚还弱小，并无足够的支付能力之时，大量人才就因其良好的发展前景和上市预期，从传统“三大”和其他主流企业纷纷加盟，呈现了一种令国内业界难以想象逆向流动的生态。

资本环境的追捧创造，必然推动了人才富有理想主义和冒险精神，而理想主义和冒险精神又获得了高回报的激励，这就构成了一个完整的正能量链条。

## 四、变局：大并购时代

2010 年起，美国整个信息安全产业格局的发展开始进入到新的大并购时代。从 2010 年 7 月开始，在之后将近两年的时间里，美国企业发起了超过 10 个价值 10 亿美元以上的并购案，其中最有影响力的无疑是“Intel 对 McAfee 的并购”，这是信息安全开始走向寡头化的风向标。美国的传统软件厂商、大集成商、芯片供应商和既有的巨头安全企业，都纷纷出手把大量独立安全公司融入体系，这些并购使其技术原有短板得以补充、新技术的储备不足获得应对以及解决方案更加完整。

我们通过图 2 展示了在大并购时代所推动的跨行业寡头体系的形成。但在这个过程中，我们并未看到这种巨型“托拉斯”所带来的垄断和对创新的扼杀倾向。

表 3 美国企业发起的信息安全相关的典型并购案例

| 时间 | 收购方 | 被收购方 | 交易金额 | 被收购方情况和其他备注 |
|---|---|---|---|---|
| 2010.8 | Intel | McAfee | 76.8 亿美金 | 反病毒业界传统巨头 |
| 2012.8 | Cisco | NDS | 50 亿美金 | 安全传输和分发方案厂商 |
| 2004.2 | Juniper | Netscreen | 35 亿美金 | 硬件防火墙领导厂商 |
| 2012.7 | Dell | Quest Software | 24 亿美金 | 企业级安全软件开发商 |
| 2010.9.13 | HP | ArcSight | 15 亿美金 | 日志和时间分析服务厂商 |
| 2006.8 | IBM | ISS | 13 亿美金 | 著名安全扫描服务厂商 |
| 2010.8 | Symantec | VeriSign | 12.8 亿美金 | 著名电子认证厂商 |

恰恰相反，这些并购多数并不是基于扩大市场份额、消灭竞争对手的考虑，而更多瞄准单点上有突出技术优势的以及能够弥补、或强化收购者自身短板的企业。被并购的新锐技术团队，多半因其技术优势而获得了良好的溢价，几人、十几人的小团队都可因其核心技术能力，获得千万甚至数亿美元的估值。从而使收购成为良好的技术创新团队自我价值实现和风险投资者的推出通道，并引发了“从寡头中再次创业，再次被寡头收购”的风潮。

因此，大量并购不但没有消亡了美国在安全领域中的基础创新能力，反而使之成为了技术创新的动力源泉。

而在国际博弈中，来自欧洲、日本、印度等国的个性安全企业，则往往在崭露头角后，被美国巨头厂商兼并。从这些企业团队角度来看，已经达成了某种成功（但交易中的议价能力往往有所不足）。但从国家能力对比来看，则汇入了美国对单极世界主导地位不断被强化的趋势。

而反之，如果被收购的是美国厂商，而买主来自其他国家。美国官方和民间机构，则会陷入异常的敏感之中，美国官方所形成的《An Analysis of Chinese

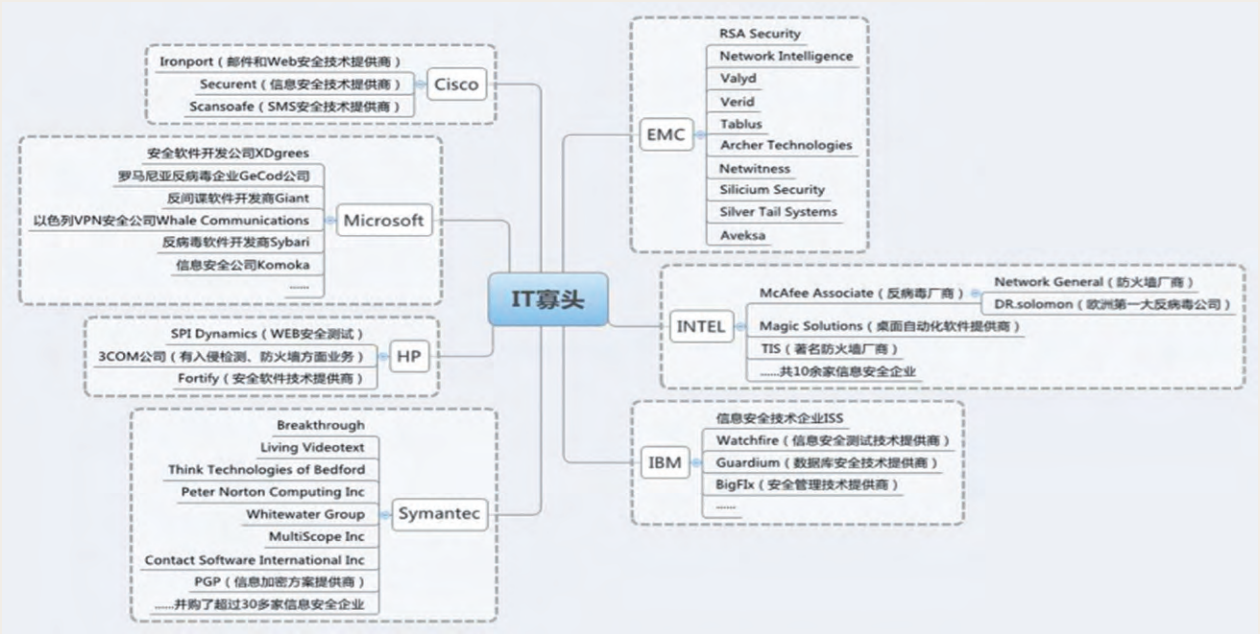


图 2 美国 IT 寡头对网络安全企业的兼并

Investments in the U.S. Economy》一文中虽然轻描淡写的说：“对于中国的国际直接投资，美国政府并没有统一的立场。国家和地方官员寻求增加经济活动以吸引中国的国际直接投资……同时，其他联邦官员极其担心中国的国际直接投资在国家安全和经济安全方面的潜在影响。”

但如果这种投资涉及网络安全，则基本不可能达成，2011 年初，美国外国投资委员会阻碍华为收购小厂商 3Leaf 的案例，就是这种紧张感的典型案例。

中国企业在美国的并购动作，显然会触痛美国政府最敏感的神经。但如果认为这种紧张感仅仅是针对中国的，其实就误读了美国固有的“国家安全情结”，一个鲜明的例子是，即使对于同在西方阵营的小老弟以色列，美国也同样做出了阻碍 Checkpoint 收购美国著名开源安全厂商 Sourcefire 的举动。

## 五、产业秩序：互信与互动与产业联盟

2011 年的 RSA 展会上，新兴的主机安全厂商 Bit9 打出了对巨头厂商 McAfee 的攻击性广告，但这其实是美国式的技术幽默。McAfee 无疑会警惕 Bit9，并视其发展做出对应的反应，但不会是那种“东方式”的强势打压。

自由竞争是美国企业发展的核心动力，这种动力中既有价值导向，也有规则定义——鼓励竞争、鼓励创新、限制垄断。这种厂商间既存在合作，又存在互补、互信的一个良好例证是——基于各自的云化服务，美国已经形成了一个反 APT 作业的“事实联盟”，在这个体系上，有 Palo alto Networks 所贡献的可执行文件鉴定服务、Wildfire、Bit9 所贡献的海量白名单和文件信誉鉴定、已被 Google 收购的 Virustotal 提供的多引擎对照扫描 + 静态分析 + 动态执行服务、Fireeye 提供的文档格式溢出和移动应用鉴定服务，而一些新锐移动云端安全服务厂商如 Trustlook、Virtual Threat 等亦可能成为体系的一员，各厂商间购置对方的分析服务，作为自身分析能力的扩展，同时还有 Solera 等厂商兼容各家产品进行集中分析，Mandiant 等则负责传播造势，从而形成了一个应对 APT 的产业资源体系和事实上的利益同盟。

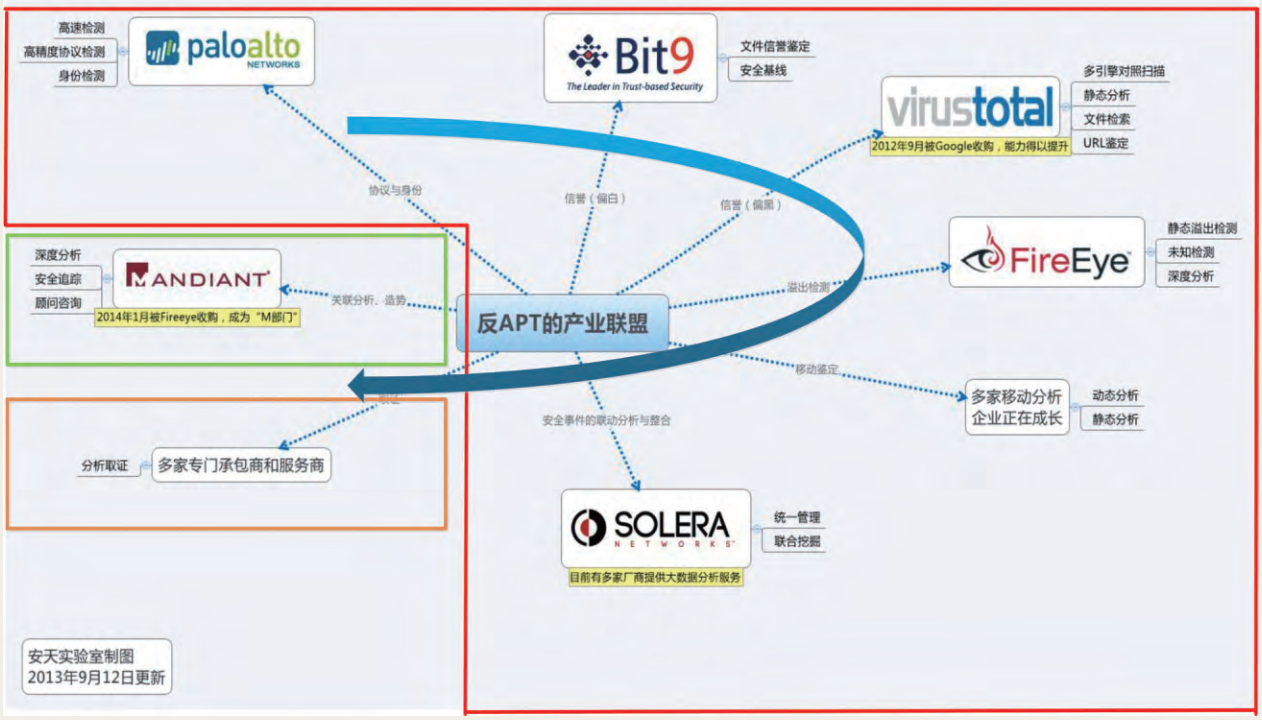


图 3 美国企业在反 APT 上的协作

## 六、政商关系解读

对于美国 IT 企业与政府间的关系，有两种意见都是偏颇的，一种是全面拔高其 IT 企业的道德操守和信息自由信仰，而对其与美国国家机器间的互动关系视而不见；而另一种则堕入彻底阴谋论，把一切美国 IT 产品都简单视为具有主观恶意的逻辑炸弹，亦把一切美国 IT 厂商都视为其情报体系的紧密互动层。而抛开这两种先天偏见，则有助于我们理清美国安全厂商与政府的微妙关系。

例如有人以德国《明镜周刊》报道的“NSA 的 ANT 系列信息装备”作为美国安全企业为美国情报机构安放后门的证据，但经过对相关资料的分析研判，更准确的表达应该是有多家安全产品的弱点可以被 NSA 利用，这里需要注意的是“弱点”和“后门”有本质的区别，否则就很难理解为什么中国厂商华为也在这份名单之上。笔者认为，这个案例总体上只能说明 NSA 信息武备的丰富程度和强大的弱点与漏洞挖掘能力。

我们从斯诺登事件引出的信息中，亦可做出下列分析：

1. 与美国情报机构建立密切关联的多数企业是有信息聚合能力的互联网巨头，由于其建立在全球用户以信息上载、聚合以及置换免费服务的模式基础上，美国可以通过爱国者法案对其数据实现“合法”监控。

2. Cisco 与 NSA 的密切联系可以被证实，但并不能说这就代表了美国情报机构与其网络设备和安全厂商的典型关系，NSA 可以放心与 Cisco 合作的原因，是后者已经建立起了全球市场的牢固不可替代性，同时其产品覆盖能力也有足够的战略价值。而其他美国厂商并不具有足够的政治风险抵御能力。

3. 美国已经通过类似标准污染的方式（类似 NIST SP800/90 标准中对随机数强度的弱化），实现对更多产品的“上游感染”，而不需要直接和这些厂商发生情报作业的关联。

笔者愿意做出这样的判断，在全球范围普遍性的

伤害美国企业的用户信任力，并不符合美国国家利益的最大化。换言之，美国在信息领域的战略威慑能力，首先来自其产品与服务的到达能力和覆盖程度，而不来自其中是否有可利用的后门。这种态度不是期望为美国专业安全厂商洗白，而是希望大国博弈的因应之策建立在理性的思考和分析之上。

我们不妨看棱镜门中的一个事实，在美国的互联网大佬中，Facebook 是最后一个加入的，同时也是棱镜“上榜”企业中最后一个上市的，而尚未上市的 Twitter 则根据资料显示尚未加入。如果做一个类比来看，这可以称为 “把羊养大了再挤奶”的原则，而不是“把猪养肥了再杀掉”。

而通过 NSA 向 RSA 公司支付 1000 万美元，换取其使用有后门的算法的操作，我们亦可以做出这样的判断，美国政府积极地为那些承担国家义务的企业提供补偿。另一个案例或许也能为这种判断提供注脚，当美国政府要求 Fireeye 对中国禁售的时候，也同时设定规范，要求与五角大楼等政府机构有网络连接关系的军火商、大的 IT 厂商部署反 APT 产品，这种导向形成了在其“爱因斯坦”计划之外的一种单点但有效的反入侵能力层次，推动了以 Fireeye 为代表新锐厂商的产品部署，而从客观上，这构成了要求 Fireeye 放弃中国大陆市场的经济补偿。

## 七、启示录

网络信息安全早已不是实验室技术，其在本世纪初就进入了以大产业体系为基础，以企业创新为动力的时代。可以说没有产业就没有技术与产品，而没有企业这个基本元素，也就谈不上产业的存在。经济界已经充分认识到中小企业是创新与社会发展的核心动力，而在信息技术领域，我们却依然期望简单地通过大规模的国家投入或是某个应用方向赌博式的技术绕前就可以改变当前的被动局面。

美国信息安全产业的强大，为我们正确理解信息化和网络安全之间的关系提供了典范注解。国内有部分声音认为，依靠信息系统的国产化和信息系统某些安全特性的增强，就可以一劳永逸地抛弃所有的安全风险、威胁和积弊，而不再需要安全产品的保驾护航。而事实上我们看到，作为拥有最高“国产化”率、最好的核心技术自给能力的美国，自身也同样面临着广泛的安全威胁，也拥有着最为发达的信息安全产业。这说明，强大的自主信息化和强大的自主网络安全互为保障，相辅相成，不可能互相取代。

美国信息安全产业的层次结构、价值导向、运行规则等，显然值得我们分析、研究、借鉴。

充足的内需是美国信息安全产业得以发展的基础，美国用户在信息时代发展中享受了最先进的技术成果，也同时深刻感受到了安全威胁，从而认识到了信息安全产品和服务是一个独立的市场门类和层次，这个层次不可能依靠信息体系自身内置的安全能力所取代。这种认识促成了信息安全产品采购在信息化的预算中长期超过 20% 的高比重，这为美国安全企业形成了充分的收益空间。

活跃的资本力量和成熟的资本市场则为美国安全厂商提供了助跑和催化机制，其对风险、收益、创新的成熟理解，促成了保护创新、引导创新的价值导向。从 Fireeye 亏损 3000 万美元上市，却能因其技术方向、产品能力和人才储备等因素获得极高的市值，我们就能看到美国证券市场的特有魅力。而 CIA 背景的 In-Q-Tel 模式的横空出世，这代表了美国官方直接入局这一领域，为美国国家安全孵化出未来所需的技术支点。

清晰的市场规范、对商业文明和契约精神的成熟理解、合理的政商关系设计等等，则都成为美国信息安全产业有利的保障力量。从而使“鼓励创新的中小安全企业发展，遏制垄断对创新的伤害”成为社会共识。

在大国竞技中，跟跑者未必要对领跑者亦步亦趋，但需要分析领跑者的领先轨迹。这种轨迹中有无法模仿的先发优势和地缘特点，以及历史经纬的偶然眷顾；但同样会有因果清晰的必然规律。认识到这些，对于跟跑者的路径选择，至关重要。（本文以作者在中国计算机学会 YOCSEF 举办的“中国网络空间战略，呼唤什么样的顶层设计？”特别论坛上的同名发言录音速记稿为基础，进行了较大篇幅的整理改写。感谢我的同事 Billy、Angel Li、雪之梦等对本文的贡献。）