独立安全厂商兴起
是中国走向网络强国的前置保障

安天实验室 / 肖新光

编者按：在开放的网络空间，每个国家既需要参与国际循环与竞争，也需要可靠的关键卡位防御能力。这也正是独立安全厂商的核心价值。美国就拥有独立安全厂商星群。比如，反病毒起步、已经成长为巨人的“赛门铁克”，以及在国际舆论中扮演重要角色的“曼迪昂特”。而以“卡巴斯基”为旗帜，俄罗斯形成了自己的战略卡位能力。其先进的反病毒引擎核心技术有目共睹。尤其是其对震网、火焰等病毒的快速跟进，将美国攻击行为完整展示于世界面前，已然是俄罗斯国家战略竞争能力的标杆。面对从网络大国到网络强国的伟大梦想，我们不禁要问，中国的“卡巴斯基”又在何方？

引子：何谓独立网络安全厂商

从盈利模式上看，其以为用户提供安全产品和服务作为获取收入的主要（甚至是唯一的）方式，从商业契约上保证了其不能滥用其产品能力和权限，使其具有以用户安全利益为最大化、以安全威胁为唯一敌人的单一价值观。

从治理结构上看，其在寻求风险资本投资为助推的同时，更立足于自我渐进发展，其核心治理团队有着高度的话语权，这使其在当前互联网产业已经出现明显的寡头化、阵营化和恶性竞争化的环境中，可以不受裹挟，保持客观和中立，既有独立、公正的立场，当然也有缄默的自由。

从地缘背景上看，其在追求产品全球化的同时，因其所处行业的特殊性，不可避免的具有民族性、地缘性的特点，其发展轨迹必然与地缘经济发展高度重合，从而可以成为国家安全利益的可靠保障者和立场同盟者。

这些特性使独立安全厂商有别于同样进行网络安全服务的互联网公司、大的 IT 厂商以及国防机构的承包商等，从而可以构成一个独立产业层次和力量。

在美国，硅谷独立安全企业圈星群闪耀。其既有 Symantec 等传统安全巨头，也有 Fireeye 这样的超级新锐。在其辉映轨迹中，类似 Netscreen、Fortinet、Paloato Network 等完成概念接力、迭代创新的过程更成为业界经典。从而形成了美国信息产业体系中一个鲜明的层次。在我们的近邻俄罗斯，以卡巴斯基为代表的安全厂商，凭借其历史底蕴和核心技术，也已经成为俄罗斯国家网络安全战略中的关键卡位点。

这些都为在中国走向网络强国的历程中，如何完成产业和技术层面的安全布防、建立保障提供了参考和示范。而同时我们也忧心地看到，中国的独立安全厂商有在信息化大格局下被边缘化的风险。我们必须重新定义价值，思考新的道路。

一、从中美网络博弈复盘看安全厂商价值

斯诺登事件曝光出的相关信息，让国内舆论陷于浓重的心理焦虑之中。对美国滥用供应链主导优势的恐慌，几乎压倒了对其他所有问题的关注。在这种语境下，完全打造一个自主制造的闭合信息产品供应链体系和信息链循环既能扭转攻防态势观点，自然也易于被很多人所接受。

这种道路选择是否符合客观规律，暂且不论。但首先应看到信息的自主性和信息系统的安全性本身就是有关联但并不相同的两件事情。自主的信息化则只是降低了在产品层面带有主观恶意的可能性，但并不必然会改变攻防态势，信息化的程度的提升，存在不断带来新的安全威胁的必然性。唯有有针对性的建立防御的层次、手段和技术，才能真正而快速的改变攻防态势。

而从另一个意义上来看，国内对斯诺登事件的分析跟进，只是此前中美网络安全战略博弈中的后半程复盘，更多是在战略态势从中方完全被动到趋向平衡后的反弹式的表达。而之前中方处于高度被动的前半程，以及这

种被动的原因，反而遭到了忽略。

这个前半程从美方炒作“蓝翔技校”等的零星指责起始，而以 2013 年初 APT1 报告发布为高潮，如果我们把 APT1 报告发布所引发的系列连锁反应进行一个图示整理和分析的话，我们可以以产业的视角，获得一些此前被忽略的信息。

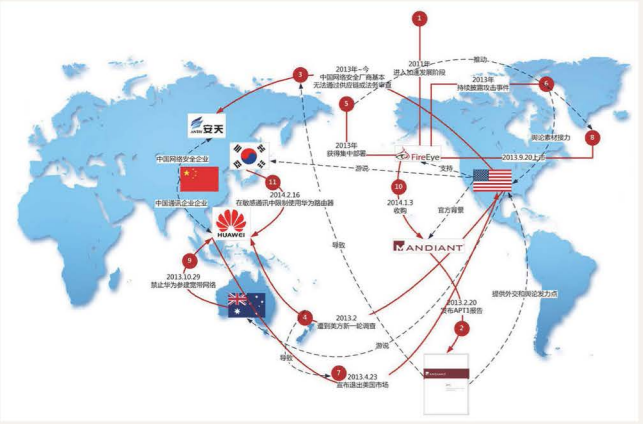

图 1 APT1 引发的链式反应的图示推导

APT1 报告发布的一个重要产业背景因素在此前被忽略了——以 Fireeye 为代表的美国新兴网络安全厂商，已经在 2006 年开始的缓慢造势中，获得了发展加速度，而其产品和技术已经具备了对抗新威胁的能力。这批厂商的进一步快速发展壮大，需要战略级别的高势能助动。

从 APT1 报告的发布时机上看，其正在 RSA Conference 大会之前。这个一年一度的全球信息安全业界的大聚会，今天我们回看时，方意识到它其实一直是的美方完全主导的话语权舞台，是美方单向表达的秀场，这种表达既是政治博弈的体现，但也是推动美国安全厂商壮大发展的造势场。

在 APT1 引发的连锁效应中，其产业层面的关联后果被政治层面的被动尴尬掩盖——华为宣布主动退出美国市场，并先后在欧盟、澳大利亚、韩国受阻；安天等已经走出海外、或者进军海外的中国安全企业受困于供应链审查，而不得不退回原点。

而 Fireeye 则迅速获得大量用户，并赢得了美国政府机构和大厂商（包括大的 IT 寡头和军工集团）的集中商业部署，这些部署一方面补偿了 Fireeye 对中国禁售的全球市场损失，也让 Fireeye 有了更强的事件捕获能力，从而可以完成对 APT1 报告的后续的“接力式”的事件披露和表达。而这种持续表达则让中方处于持续的态势被动之中。

Fireeye 本身则不仅成功完成上市，而且随着快速发展，迅速跻身市值突破百亿美元的公司行列，甚至有资深业内人士预测，其有可能在市值上超越美国传统巨头 Symantec，成为全球估值最高的网络安全公司。Fireeye 的迅速崛起，同时带动一批新型美国安全企业，纷纷获得估值上的持续成长。

这种产业能力的此消彼长，是大国竞争中的实质损益。而如果还认为上述产业层面的关联推导显得牵强的话，那我们且看 2014 年 1 月 Fireeye 以 10 亿美金的价格收购了 Mandiant 所释放的信号，这不仅是在产品能力和分析能力的强强联合与互补，同时也构成了“借力者”对“造势者”的“投桃报李”。从其更深的背景来看，更是具有美国特色的政商关系中的一个典型而成功的“旋转门”案例（Mandiant 具有鲜明的美国军方的背景）。

从上述复盘可以看到，美国安全厂商技术能力培育出的政治花朵，最终让美方结出了综合的产业果实，而让中方吞下了产业苦果。中国在网络安全角度战略被动的直接原因，正是美国通过其安全企业能力，有效发现、长期跟踪和深度分析了被认为来自中国的攻击，并提供了相对完整的证据链条和推理过程。而中方既没有对位能力发现和深度分析来自美方的攻击，对等爆料；也没有通过具体和有针对性的技术分析，有效反驳美方的指责。导致了美方可以尽情单向表达。并且通过其全球舆论控制能力长期占据的价值观高点，在国际舆论层面成功完成了对“西方世界是网络攻击的唯一受害者”和“中国是全球互联网安全公敌”的通俗观点包装。

通过美国安全企业的技术能力发力，并在政治层面借势而为的手法，既让美国产业界直接获益，亦为美国官方赢得了可进可退的作业空间，体现出了美方的综合战略布局的层次感和战略博弈的实力与技巧。

这一复盘所展现出的是：具有先进技术、创造力和勇气的安全厂商，在大国战略博弈中，不仅有是技术和战术层面的价值，更具有战略性的价值。

二、优先推动安全厂商发展是快速改变战略态势最优选择

面对复杂的国际战略竞争形势，中国在信息产业发展上，逐步立足自主可控，具有一定的必然性。但亦应理性认识到，在供应链全球化（而美方把持上游）、信息链单向化（全球数据向美方聚合）的大背景下，没有任何国家可以同时做到既收获全球化的经济果实以实现国家发展，又通过打造闭合的供应链和信息链来保证国家安全。更何况，高速发展才是最大的安全保障。在这种交织复杂的体系中，中国的国家利益最大化绝非自我闭合，偏安一隅，而应是通过产业能力的发展，逐步与美国分享全球供应链和信息链的主导权。

美国是信息技术世界单极霸主，在自主与安全可控问题上，它的现状或者能给我们一些思考，美国通过微软、谷歌、英特尔、高通、甲骨文等公司完整把持了操作系统、核心芯片、数据库等关键 IT 环节，同时通过新兴互联网巨头们形成了对全球数据的有效聚合。但这种空前的自主性优势，并没有消减美国整个网络体系和信息系统所具有宽大的攻击面（Attack Surface）的隐患，其遭到各种入侵攻击的事件依然此起彼伏。

而迅速改变其防御态势的，反而是快速部署 Fireeye 等相关产品形成的独立防御层次；以及依托 APT1 等报告和 Fireeye 系列报告所展现的分析能力和舆论威慑。

因此对国产关键信息系统的自主国产化的关注，不应冲淡和忽略了直接的对位防御能力和产业层次的建设。唯有在自主可控的路线选择上优先保证网络信息安全产品的研发自主、安全可控与技术先进，才能在供应链和信息链中，快速建立安全卡位点。唯有让中国安全厂商快速形成针对外方对中方攻击的有效捕获、关联分析和取证溯源能力，持续形成分析案例，才能为大国网络安全规则的话语权博弈积累表达素材，有效遏制美方的单向表达。

因此推动网络安全厂商的发展，在当前被动态势下，是最具针对性的选择。

我们通过数据来观察 Fireeye 与 Mandiant 这两家已经合为一体的企业，我们发现 Fireeye 尽管 2013 年风光无限，但全年的营业额只有 1.6 亿美元（预计 2014 年会有较大增长），从营收上并非巨无霸企业，而 Mandiant 营收可能更少。而更值得思考的是，其都是在 2004 年创立，其历史比美国主流 IT 企业要短得多。而其快速发展则只是最近 3 年左右的事情。因此布局于网络安全厂商的发展，不仅可以实现四两拨千斤的效果，亦具有更低的时间成本。

	Mandiant（曼迪昂特）	Fireeye（火眼）
股票代码	未上市	Nasdaq: FEYE
创立日期	2004 年	2004 年
地点	美国	美国
总市值（美元）	2014 年 1 月被火眼用 10.5 亿美金（股票 + 现金方式）收购	89 亿
2013 年营业收入（美元）	未公开	1.6 亿
2014 年预估营业收入（美元）	2.5 亿	
在职员工总数（参考，2013）	未知	320
产品 & 服务线	Mandiant Managed Defense™ Mandiant for Security Operations™, Mandiant for Intelligent Response ® (MIR ®) Incident Response Services Mandiant Intelligence Center™	Web Malware Protection System Email Malware Protection System Malreware Proteciton CloudFile Malware Protection System Malware Analysis System Central Management System

表 1 Mandiant 与 Fireeye 的企业情况

基础信息技术环节的成熟完善，是一个漫长、投入巨大的过程。以操作系统领域为例，微软公司在 Windows Vista 的研发资金就已经超过 30 亿美元，而其庞大的安全和应急响应团队，更是通过高成本、高质量的运行，为 Windows 系统和微软生态体系提供安全保障。这种投入能力不是一次性的，而是以企业持续发展为基础的持续投入能力。而这种长期投入积累也形成了空前的技术落差和壁垒。

而在安全产品和安全技术方向，总体来看我国与发达国家差距较小，更易于发力短程集中投入、打造高点优势的成本，则相对较低。以安天自身为例，在移动安全领域，安天集中兵力研发移动反病毒引擎，通过技术路线的正确选择、研发团队的积极努力和有限的国家资金支持，仅通过不到四年的时间，仅以千万量级资金的投入，就在 2013 年以全年平均测试的第一名的成绩，摘得了德国权威测试机构 AV-TEST 的移动设备最佳保护奖，实现了中国乃至亚洲安全厂商在欧美权威测试机构年度奖项零的突破，为近亿部手机中的安全产品提供了中国制造的安全核心技术。

显然，通过安全企业完成卡位也具有投入绩效比的经济性。

我们的近邻俄罗斯，在优先保障网络安全企业发展方面，已经走在了我们前面。

俄罗斯虽然有高水平的信息技术人才基础，但在基础信息环节上，除了 Linux 发行版 Ubuntu 系统外，基本乏善可陈，与中国类似，其同样是信息大国，但和美国相比，远不能称为信息强国。但其给予了以卡巴斯基为代表的俄罗斯反病毒企业群体充分的支持，从而形成了从核心技术到分析能力的高地。卡巴斯基在 Stuxnet（震网）、Duqu、Flame（火焰）等系列具有美国背景的 APT 事件中的分析表现，敏锐而深入。而在全球一些分析团队陷入 Flame（火焰）蠕虫的分析长跑之时，其又独家爆出了与之相关的另一组恶意代码 Guass（高斯），显出了其深厚的技术能力和素材储备。这种能力显然是俄罗斯争取大国网络话语权博弈，以及在网络情报与网络交战原则博弈中获取有利位置的有利支撑。

因此，快速推动独立安全厂商的发展，能够快速而低成本的改变攻防态势，建立产业屏障，既有其路线的合理性，又已经被他山之石所证明。

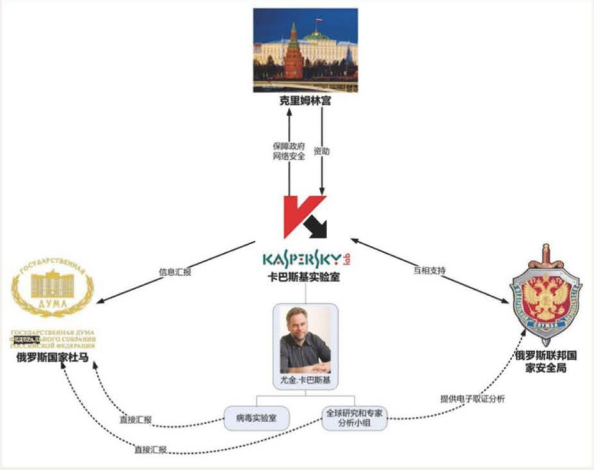

图 2 卡巴斯基的在俄罗斯国家安全防御中扮演的角色

三、中国独立安全厂商的生存危机与未来导向

当前，中国网络安全厂商已经面临着严重的生存危机，这种危机既有因内需不足所导致的业务上的发展缓慢，同时也连锁导致了发展乏力和空间压迫所带来的人才枯竭。

中国安全厂商，从人才上正陷于四面围堵的状态：

互联网寡头公司对安全人才不遗余力的吸纳，让国内安全企业正在逐步丧失招聘一流人才的能力，其培养出的人才亦大量迅速流失，在互联网巨头们纷纷提出了建设网络国防的基调下，中国安全企业的人才根基被迅速动摇，大量优秀的安全工程师成为寡头企业的“私人保镖”。

同时，庞大的地下经济由于缺少综合治理，不仅制造了大量的安全威胁，对安全工程师团队也起到了腐蚀作用，导致一些安全人员滑落到对立面，这种轨迹令人痛心疾首。

国家对信息安全方向的大量投入并没有充分从采购上盘活内需，而是更多流入了高校和科研院所，信息安全方面的基础研究固然重要，但国家安全能力必然最终要以产业为依托，产业则以企业活力为动力。而中国高校如今处于不是为安全企业培养人才，而是与安全企业大量争夺工程性人才，以完成科研课题和社会项目的状态。

在大洋彼岸，硅谷安全公司也凭借宽松的研发环境，良好的薪酬待遇、居住环境等综合条件，亦包括美国所处的价值观高点，通过工作签证的方式，又让大量的国内顶尖安全研发人才向海外流失。

而从中国安全厂商自身来看，部分厂商在困局之中看不到破局的希望，创新动力匮乏，更多地选择跟随、模仿、抄袭，缺乏突破核心技术的勇气。甚至凭借已经拥有的用户信任和资质，贴牌国外安全产品或使用国外反病毒引擎，并把这种伪国产产品，销售给敏感单位。

上述危局的形成具有必然性，但如果我们予以有效应对，也同样具有反转的可能。

当前隐私、安全等概念已开始逐步在国内个人用户层面深入人心，但获得安全保障需要付出必要的成本，尚未形成全民共识，这必然导致网络安全并非刚需，也将进一步导致中国网络安全市场在很大程度上成为一个关系性的、而非需求性的市场。但刚性需求不一定由自发形成，也可以由引导和规范来推动，逐步形成用户，特别是行业、企业用户对网络安全的刚性需求是安全厂商发展壮大的根本动力。

此前由于内需不足，但同时又需要保证安全企业得以生存发展，国家通过创新基金、863计划、发改委信息安全专项等政策对安全企业提供了支持，这是必要的，但不可能是长久的，企业发展必须依靠真正的市场来解决。而目前有限内需实际又部分被行政门槛和行业壁垒等瓜分掉。在一些局部领域，甚至形成了技术和产品能力上的负淘汰。因此形成良性市场秩序才是安全厂商迅速发展壮大的根本保证。

而上述过程亦需时日，参考美俄的做法，选准具有自主研发能力、创新精神与国家安全价值认同的民族安全企业，对其进行必要战略扶植则是安全厂商大发展的重要前提。

而逐步在博弈中达成大国间网络情报作业和网络交战原则，形成新的战略平衡，将有助昂于各方立场回归理性。也会使中国安全厂商重获进入发达国家市场的机会。而中国的外交战略引导，应该也可以为中国安全厂商进入亚非拉市场带来便利。为中国安全厂商国际化创造条件，则是其发展的进一步空间支撑。

任何外部环境的因素变化，均需要时间和过程，对于依然在艰难跋涉的中国独立安全厂商和希望走入这个行业的创业者们来说，改变命运最终还需要依靠自身的智慧、坚韧与自强。

尾声

张文木先生在《世界地缘政治中的中国国家安全利益分析》一书中将“独立完整的主权，统一的民族市场和有独立研发能力的国家战略企业”称为民族国家的三大支柱。并进一步指出“国家主权是技术产权的政治保证；民族市场是孵化和试验技术，尤其是国家战略性技术的基地；而独立的研发能力是保持国家科技、尤其是战略性科技在国际上的领先地位的最基本的前提”。

中国正走在从网络大国到网络强国的道路上，正处在“没有网络安全就没有国家安全”的全新时代中。现在是中国独立网络安全厂商集体站出来，成为真正意义上的国家战略企业，肩负起产业结构层面和战略态势层面的双重屏障责任的时候了。

（感谢我的同事 Angel Li、Billy 等对本文的贡献）