中国网络安全产业的困境、症结和希望

■ 安天实验室 / 肖新光

编者按：本文是作者在本刊 2014 年 3 月号发表的《独立安全厂商兴起是中国走向网络强国的前置保障》一文的姊妹篇。

一、网络安全产业的困境

“网络安全”现状的不容乐观，是中国作为网络大国却不能被称为网络强国的原因之一；“网络安全”的能力完善，是中国作为网络大国走向网络强国的必备支点。

如果这两个判断没有错，那么我们就会发现中国在“网络安全”这四个字上，存在着很多令人深思的矛盾与悖论：网络与应用蓬勃发展，网络安全尽管在其后奋力追赶，但距离却似乎越拉越远，成为掣肘；我们看到了网络安全似乎被空前的重视，却不得不面对小得可怜的信息安全市场空间；我们听到了很多人都相信这个产业未来的前景，但又无奈地感叹眼前并无发展良策。作为一名“网络安全”产业的从业者，作为技术的研发者，我们置身于这些矛盾之中，虽然也有着很多惶惑和不解，但我们在从“学艺”到“卖艺”蹒跚而艰辛地行走二十年后，却依然未能带给用户、

带给国家有底气、有扎实基础的安全感，亦深感愧疚。而在惶惑愧疚中，我们也在以自己的角度思考着未来。

今天中国数以亿计的用户，依赖网络进行着生活与工作；数以千万计的政府部门、机构、企业和法人实体，依托网络和信息系统进行生产和管理。对于国家的现代化和信息化进程来说，信息化已不再是“可选项”，而是空前的成就；而从网络安全角度来看，这是一个巨大而且决不能失守的防御阵地，也是一个复杂的作业纵深。试图完全梳理这样一个复杂的、多层次的巨大系统的威胁全景，无疑需要更长期和细致的工作。几乎所有“网络安全”行业内外人士都认为，面对严峻的安全挑战、面对从地下黑产到带有国家背景的复杂威胁，这个体系中的任何目标都处于危险之下，这样的一个又一个的弱点，组合成一种安全困境，带来了极大的恐慌感。这种恐慌感，既是对真实情况的本能反应，又有因各种意图不断放大宣传“斯诺登效应”而给受众带来的自我恐吓。

焦虑引起认知失调，巨大的挫折感引起应激行为，在网络安全产业，具体表现为在没有全面系统的威胁分析、没有进行针对性的对手分析与沙盘推演的情况下，网络安全厂商的安全手段和环节便开始受到更多的质疑和不信任。这种不信任深深地萦绕在网络安全的困境与迷雾当中。

网络安全是永恒的对抗博弈，这本来是最能明显体现辩证法的“对立统一、斗争和运动、普遍联系和变化发展”基本规律的场景，如今很多人却在高度信息不对称的情况下，因对威胁的恐惧和对对抗的厌倦，而广泛产生对“一劳永逸”解决问题的不切实际的期待。从各种“安全永动机”到“自闭合供应链”，一枚枚“银弹”被绘制成愿景蓝图，在这个被描绘成“后门无所不在，敌人也无所不在”的体系中，大家忘记了其实安全防护的基础工作还有很多提升的空间，大家仿佛觉得一切现有防御机制已经失去意义，一切体系必须推倒重建，否则就不能达成其安全。其中不仅包括安全环节，甚至也包含了既有的信息化进展。

在这些林林总总的质疑中，以质疑网络“老三样”（防火墙、反病毒、打补丁）没有价值，最为普遍。这些传统安全手段在对抗 APT 等新威胁中，确实力不从心。但如果我们真实地对政企网络进行深入分析了解，我们会发现，在大量政企网络中，已经采购的防火墙通常并未加电或者未经过有效的策略配置，反病毒产品只获准数月甚至半年升级一次，而更多业务系统的管理者“不敢”打补丁。老三样，是没有用？还是没有被有效使“用”？这三个环节，是无效环节？还是没有被做好（当然包括开发者的责任）的必备环节？随着 APT 等新威胁的发展，网络安全的能力纵深必须得到有效延展。但无论从投入还是管理角度，“补课”同样也是网络安全管理中的重要环节。

一个有趣的故事是关于美国当今网络空间能力代表厂商 FireEye 的。某巨头厂商依托已知二进制可执行样本集合对 FireEye 的产品进行测试，发现检出率只有 1/5 左右。这个小规模的内部测试在国内引起了思考，有人迷惑这样的产品价值何在？这个检测结果是否与 FireEye 的用户期望匹配？但其情况就是，FireEye 产品并不是用来替代现有防火墙、UTM 或者其他安全产品的，其专注于解决 0day 与高级威胁，并与其他成熟的安全环节和内网管理能力相对接，形成了安全的能力纵

小链接

银色子弹常被用做致命武器的代言词。被比喻为具有极端有效性的解决方法，作为杀手锏、最强杀招、王牌等的代称。在 IBM 大型机之父佛瑞德·布鲁克斯（Frederick P. Brooks, Jr.）1986 年发表经典论文《没有银弹：软件工程的本质性与附属性工作》（No Silver Bullet — Essence and Accidents of Software Engineering）

深和延展。FireEye 的产品不是“银弹”，任何今天的和未来的产品也都不会是“银弹”，因为网络安全没有“银弹”。但就是这样一个同样没有“银弹”的厂商，却毫无疑问是有实力影响大国博弈格局的支点厂商。

在网络空间的大国博弈的进程中，笔者此前文章曾把“斯诺登事件”看成一个微妙的分水岭，斯诺登事件之前，美国频频曝光所谓的网络安全威胁，中方反制乏力，但国内安全业界有识之士们也在知耻后勇中，积极蓄力。而斯诺登之后，从国际舆论斗争上，中方赢得了短暂的战略喘息期，但对建立卡位能力和反制能力的迫切性认识骤然下降，反而在一种巨大的基础设施恐慌中，开始了信息技术环节各点的全面“大跃进”，而这种大跃进中不乏号称“能解决全部现有安全问题”、“杜绝了攻击”的新思路。在美国的国家信息安全防御体系依然倚重被严谨配置使用的“老三样”所带来的基础安全防护能力时，我们的眼光已经超越了美国在基础安全防护上采用的新形态增强防护技术，尝试跨越式地探寻解决一切安全问题的“银弹”技术或方案，同时完全无视在信息化与信息安全严重不平衡发展过程中欠下的“账”。

随着斯诺登的“猛料”开始渐渐减少，随着人们对其新鲜感的下降，可以看到美方从企业到政府，对“中国网络攻击”问题上的指摘表现再趋活跃，而很难想象还会有下一个“斯诺登二世”的出现。令人深思的是，真正“收容”着斯诺登的俄罗斯，在国际外交局势的困局中，却由其标尺性安全企业，打出不依靠“爆料”的真正的“硬牌”——卡巴斯基安全实验室在 2 月 16 日起发布《Equation: The Death Star of Malware Galaxy（方程式：恶意代码星系中的死星）》，揭露了带有美国官方背景可以通过硬盘固件实现持久化的攻击组织“方程式”。而此后的一个月内，当国内各界以此为一个新的传播红利进行消费的时候，卡巴斯基又连续发布了四篇深度跟进分析。报告所体现的是卡巴斯基的全球产品能力和深度分析能力。“为什么又是境外厂商抢先发现曝光了威胁”、“中国的安全厂商为什么这么不中用”。面对这些质疑，笔者也深感惭愧，但面对“方程式”这个似曾相识的对手，却又不得不报以苦笑。

能力可以持续建设，市场可以逐步扩展，而可能令国内具有类似潜质的安全团队所羡慕的，或者还有很多更为深远的外部机制性因素。更深层次的问题聚焦于产业发展政策，以及由此构成的产业环境上。

二、产业表象与分析

中国的网络安全的希望必须首先寄托在网络安全产业的发展之上，必须有一批具有核心能力的强力企业，而这一点正在为更多人认同。但在中国互联网和信息化狂飙突进的二十年中，中国网络安全产业，并未实现同步的成长。在华为的估值已经被预测与思科等量齐观，阿里一跃成为市值第一大的互联网公司的时候，中国网络安全依然没有按照人们预期的那样诞生一个产业星群，我们看到了各种安全基地与孵化器，看到了林立的安全会议，有数以千计的企业声称自己出品网络安全产品、或从事网络安全业务，但其中既没有赛门铁克这样的巨头，又匮乏 FireEye 一样的新锐。其中原因何在？

让我们进一步分析一些表象，也再看看其中背后的原因。

表现一：自主研发与贴牌混淆、实质性创新能力不强、动力不足

国内网络安全业界长久以来一方面极力推崇自主研发、自主创新；但在具体的产品实践中，则又体现出自主研发创新能力和意愿的不足，贴牌与 OEM 在行业内成为一种通行法则。而一些有一定自主研发能力的厂商，也通过 OEM 的方式补齐一个完整的产品线，从而来扮演全能力的解决方案供应商形象。

在 2002 年前后，曾有“四大开源毁了中国网络安全的自主研发”的说法，当然这是一种黑色幽默式的反讽表达。所谓四大开源就是 IPtable\IPchain 防火墙、Nessus 扫描器、FreeS/WAN VPN 和 Snort 入侵检测。而在当时，基于对这些产品的简单汉化，使国内出现了大量“自主知识产权的”网络安全产品。当然笔者并不认为应该重新发明轮子，而不去借鉴开源的成果，但这些“自主”产品多半并未在像国际领先同行们那

样在开源基础上继续延伸创造，同时也没体现出对开源协议知识产权的应有尊重，更别说通过进一步将有价值成果开源而影响国际产业圈。当一个市场行政门槛较高、行业壁垒较多、重度依赖客户关系的情况下，一旦可以通过取巧的方式降低研发门槛的话，这种效应就会被迅速放大，网络安全领域成为了一个缺少实战评价标准的低技术门槛、高准入门槛市场，在各方面都体现出了“劣币驱逐良币”的特点。然后自然就像我们看到的那样，短时间内冒出数百家号称拥有自主知识产权防火墙或 IDS 的厂商，在同样的开源代码上进行同质竞争，其结果完全与开源作者的初衷背道而驰。

当然，由于网络安全市场的微利，当年那种“百家百墙”的局面渐进被商业竞争洗练掉了。而同时由于以北美厂商为引导的全球网络安全企业的蓬勃和发展，则为国内市场提供了更为丰富的贴牌选择。2012 年前后的一篇网文《防火墙 UTM 产品 OEM 第三方或嵌入第三方反病毒引擎利弊分析》就介绍道，大量“国产”防火墙、UTM 等网关设备实际大面积采用了境外反病毒引擎和直接贴牌 OEM 的情况，从文章所介绍情况可以看到，一些防火墙投标，其实成为境外“飞塔”等产品的贴牌战争。

对于这段大面积抄袭开源于前，广泛贴牌于后的历史，部分从业者已经感到见怪不怪和习以为常。小生产传统和地域、行业壁垒这对怨偶一旦结合在一起，在外部产品能力的冲击下，就会使多数企业自然的回避研发竞跑，而寻找关系和资质壁垒保护，从而充分造就出企业的研发惰性。而此时整个产业肌体所表现出的气质，就是丧失对外竞争的勇气，对内形成对部分尚有研发能力和意愿的团队的吸血和盘剥。

表现二：创业者队伍后继乏人，本土独立安全产业中坚力量匮乏

产业危局的另一个表现是，这个领域缺少一代 85 后、90 后的创业者阶层，尽管出现一些新的团队和品牌，但其关键发起者更多的是熟悉的面孔。

这让我们想起，2000 年前后，一批批中国的网络安全研究者和爱好者，展开了创业之旅，堪称基本与中国互联网同步起步。而中国今天几家主要的网络安全企业包括启明星辰、绿盟、安天多数诞生于那个看起来环境更为艰苦，但更为宽容，也更富有理想主义色彩的时代。网络安全工作者未必有很高的收入，但却受人尊重和推崇。而这批企业的发展与壮大，成为了中国网络安全的中坚力量。创业不仅是造就一批企业，也是造就一代的人行动。可以说，网络安全在尚未全面崇尚创业的年代，成为部分卓越青年的创业选择。而在今天，我们却看到网络安全方向很难成为青年创业的首选。

而在为数不多的安全创业团队中，我们可以看到与硅谷安全创新团队那种广泛的领域分布不同的是，国内能获得良好估值的安全创业团队，通常比较集中在个人用户和桌面上，而很少触及企业应用。另一方面，创业者团队也普遍体现出了对技术声望、技术先进性和功能丰富性的片面追求，在工程化能力方面普遍存在明显短板，这也导致了创业者们的成果难以转化为支撑国家能力。

表现三：“马太效应”驱动跨界打劫，导致独立安全厂商弱化

大的互联网公司间的安全内斗，从目前角度来看，给了中国传统的独立安全厂商巨大的压力。一方面这些厂商雄厚的财力使他们在招聘网络安全人才方面极为慷慨，不仅让独立厂商的成手流失，而且也难以获得优秀的毕业生；另一方面，把政企网络视为互联网装机量延伸的思路，又凭借免费模式进一步打压了传统安全公司的企业市场主阵地。面对这种压力，部分安全厂商认为这是一种困境和危局，而部分安全厂商则直接选择了被互联网厂商收购或控股。

但值得注意的是，国内的互联网安全厂商，崛起于互联网免费模式，而各互联网寡头也纷纷跟进，这种模式和一些国际安全厂商的免费模式是不同的。国际的免费安全模式更多的是靠个人用户免费来获取用户口碑，而在商业用户和企业用户收费的模式；而国内的模式实际上更多是迎合国内用户更在意支出成本而忽视自我权益的价值取向，以免费服务形式引导用户必须同意分享部分轻量级的隐私以及托管入口与流

量的控制权。这种模式确实是正宗的基于轻隐私聚合的互联网模式。因为从网络安全行业传统的价值规律来看，用户和厂商是依托商业合同达成的用户契约关系，而这种商业契约关系则是安全厂商不滥用特权的保障。因此这种模式与互联网免费模式间，其实有一定先天的价值观对立。比如你很难想象出赛门铁克或者卡巴斯基的杀毒产品，向用户推荐一款游戏。但在基于免费的安全服务，接受这种推荐就是用户要付出的代价。这也互联网安全厂商必须维持巨大的装机量才能保证生存，因此难免出现在用户控制权上的缠斗和相互绞杀，甚至有可能出现与灰色渠道和分发体系的“媾和”。而这显然已经与安全行业应有的企业品质有所冲突。

笔者一方面尊重互联网安全兴起，带来的技术进步与变革，同时也对此有一定的价值观疑虑。而如果对比美国的市场格局的经验看，独立安全厂商是一个重要的产业层次，其价值观通常与国家战略更为一致和统一，同时也是重要的产业监督和制衡力量。

三、产业梳理与思索

1. 盘点家底、重建自信

有研究者对于中国网络安全的产业层次格局做了类似于“阶层分析”的梳理，将其划分为在安全上有较大投入的互联网巨头、互联网安全厂商、国家队、主流安全上市企业、行政壁垒和销售型厂商与潜力型创新厂商几类，并指出最后一类具有技术突破能力的潜质厂商匮乏，是中国网络安全当前面临的主要危机。从这个梳理来看，中国的网络安全产业，可能只是一个不够良性的整体架构，但显然并非一无所有。

无疑，在当前的空间环境下，类似笔者在《大战略基石——美国信息安全产业格局的解析》中所描述的那种通用和个性厂商非常活跃的产业格局难以出现。而本该作为最活跃的力量的网络安全专业企业其实生存在国家队和互联网巨头厂商的夹缝当中，前者并不拥有网络安全领域完整的技术研发能力，也可能像无数之前的产业领域那样，并不适应需要高速迭代和竞争的产品领域。但无疑更为政府信任，因此基本获得了全部的国家预算空间，而后者则几乎垄断了高端人才，使独立厂商的运转处于非常困难的境地。

但笔者并不觉得这种局面注定悲观。以业内非议最大的互联网厂商对安全人才抽取来看，这种哄抢，在短时间内确实让独立安全厂商运行举步维艰。但确实拉升了安全人才的平均待遇，也提升了职业吸引力，从长期角度来看，会有更多青年希望加入到安全这个行业，也为安全的长远发展蓄积了可能性。从某种意义上说，这种大规模的人才拉锯战，甚至促成了硅谷和海外的人才回流。同时，BAT3 疯狂收购和控股安全厂商团队，虽然在短时间内，让具有独立立场和安全价值观的安全厂商阵营有所弱化，但一定程度上，也为盈利能力较弱的安全厂商提供了一定的资金输血。同时也为境内安全厂商，在战略能力和经济价值高度不匹配的情况下，提供了一种基本可以按照战略价值估值的可能性。互联网厂商的投资、技术资源和互联网方法的融入客观上能够推动技术的进展；而且互联网厂商日益转向资本化运作，在安全市场导向好转时，其投资的安全企业也可能成为重要力量。

换一个更为冷静的表达，国内网络安全产业，当前是一个以国家队对接主要国家需求想象，以国内互联网巨头厂商为基本生态和主要融资平台的体系。尽管前者缺少现代威胁场景下对抗博弈的基础经验，尽管后者的价值观显然与纯正的网络安全价值观有着看起来难以调和的冲突和矛盾，但这些一定程度上成为了我们审视国内网络安全现状的一种既定事实和前

提条件。

如果在 IT 本身的大变革中，依然把网络安全的症结归咎于类似 CPU、操作系统，这样的前期基础环节的话，则无疑就会发现，从 CPU 又关联到指令体系、IC 设计工具，从操作系统又牵扯出编译器和工具链，从而发现这种自闭合式的安全幻想几乎没有尽头，而且完全不可能用国家投入和有限的市场空间主宰。而把网络安全的问题放到网络安全本身来看，就可以看到在若干个单点上，中国安全厂商已经走在了前面，这一点从中国厂商连续两年蝉联 AV-TEST 的移动安全奖项就可以看到，中国安全研究者和团队其实正在渐渐打破国际网络安全技术体系的格局，尽管这种破局战略内涵没有得到足够的重视。

无论是互斗频频的 BAT3，还是能力并不足够承担国家期望的中国独立安全厂商群体，都是中国网络安全的既有基础。“一鸟在手，胜似十鸟”在林，我们必须理解现实图景，再去考虑未来的无尽可能。

2. 内需不足是中国网络安全产业根本问题

我们曾这样解读 FireEye 在上市前的情况，FireEye 是一个中等规模的安全企业，其年营业额 1.6 亿美元，与国内启明星辰、绿盟等上市企业差不多，人员 300 多人，也与国内安天等未上市安全企业差不多。这种解读的潜台词是无论从收入上还是从人员规模上，FireEye 并非不可企及。尽管上述数据没有错，这个“错位对比”掩盖了一个问题，如果以今天的汇率来看，FireEye 在其上市之前即实现了超过 300 万人民币 / 人年的平均产出。而国内网络安全企业则有着著名的 50 万定律，即百人以上的规模企业，很难突破 50 万人民币 / 人年的人均产出率。这个并不严谨的“定律”几乎成为一个魔咒。而当前国内主流的互联网厂商的人均产出率是则是数百万人民币。这个差距决定了人才的走向，也决定了网络安全当前并非技术天才们创业首选方向。

如果一个行业，缺少技术上令人欣赏、品格上令人尊敬、成长上令人鼓舞的榜样企业。那就不是某个、某几个企业的经营问题，而一定存在着整体的共性问题。鉴于短时间内以国内安全企业的规模能力和国际形势，全面角逐国际市场依然十分困难，因此我们可以把这个问题称为“内需”问题。这个内需问题的表现为：

- 规模总量有限：依据最新 CV 发布的《CYBERSECURITY MARKET REPORT（网络空间安全市场报告）》，全球网络空间安全市场 2014 年为 710 亿美元而国内目前来看只有百亿人民币左右，即使凭借考虑更多外延的计算方法，也很难超过 300 亿人民币。国内信息市场总体规模问题依然是网络安全产业发展的关键的瓶颈性因素。
- 需求刚性不足：显然在当前的政企信息化中，网络安全并未成为刚性的需求，而更多是满足合规需要。而这种需求显然刚性不足，但值得深思的是，这种刚需不足，并非是由于没有足够严重的网络安全威胁，而是在治理能力不足、安全导向模糊的情况下，已经对国内管理机构和用户形成了温水煮青蛙的效应。对比一下，在“心脏出血”漏洞中加拿大 900 组用户报税数据被攻击者获取，即被视为极为严重的安全事件，并抓捕了攻击者。而国内多个主流站点都有 T 级的内存数据流失，却被一些管理者和媒体认为，并没有产业界宣传的那样严重。而其中的事情就是，我们感知能力低下，响应能力不足，同时已经习惯了全民分担安全治理能力低下的成本，而对网络安全问题有了一种不以为然的耐受度。而 FireEye 等近期在美国崛起的新锐信息安全公司，一方面它们确实在技术能力上具有明显优势，另一方面它们也是由美国国家级信息安全需求和大国博弈的需要支撑起来的。
- 市场严重碎片化：有限的市场被大量的地域门槛、行政门槛分割后，就进一步造成了市场的碎片化和离散，更不利于与规模型企业的壮大发展。

3. 用户觉醒和导向变革是中国网络安全产业的根本机遇

有趣的是，从全局的安全产业来说，中国网络安全产业其实有一个不错的基础开局，这个开局就是在上世纪 80 年代末已经开始兴起的反病毒产业。在当年没有类似 ClamAV 这样的开源资源的基础上，亦没

有 OEM 的财力和可能，中国最早的反病毒工作者是在最直接与病毒的短兵肉搏中坚定的成长，在解决用户问题中壮大，并诞生了多家具有特点的代表企业。当然由于诸多原因，这种格局最终没有得到延续。而相比之下，同样崛起于反病毒领域的赛门铁克、迈克菲、趋势等厂商，则成为了美国网络空间安全中的巨人型企业。这个黄金时代的重要经验，就是只有厂商应对威胁才能良性成长。而只有用户重视威胁，政府有正确的规则导向，企业才有应对威胁、因需而动的创新动力。

网络安全市场内需的规模是不可能通过政策性支持或科研投入支撑起来的。通过合规要求手段虽然能够调整信息安全在信息化的投入占比而扩大市场内需，但从国际与国内的实践来看，合规推动的市场规模拓展缺乏可持续性，而且普遍使信息安全技术与产品市场出现了“良莠难辨”的低水平走向。想要真正提升网络安全市场内需、通过市场机制推动网络安全产业发展，首先需要找准网络安全市场的发展方向，努力塑造网络安全产业的正向价值链。以美国的网络安全产业发展历程来看，网络安全产业重新将政企用户作为专注重点，走出依靠安全技术吸引眼球转而以其它渠道获利的中间阶段，通过将网络安全技术与产品应用到实体经济中实现网络安全的真实价值，从而形成繁荣并可持续发展的网络安全市场。

审视国际网络安全市场的发展，我们可以发现随着网络安全威胁环境变得日益严峻，美国的政企用户在更加以结果为导向的合规压力下，对网络安全的对抗性等特点有了进一步的认识觉醒，逐步开始认可网络安全为政企机构带来的实际价值，在政策引导下渐渐开始形成较为成熟的“网络安全审美观”，开始提升对网络安全防护有效性的追求，并相应地加大对网络安全的投资。随着政策导向的变革与用户的觉醒，我们观察到国际网络安全市场规模快速增长，而越来越多技术专精的创新型企业在普遍低迷的经济环境中逆势成长，网络安全市场逐步进入良性循环。

反观我们的网络安全市场，大量企业在“良莠难辨”的市场中苦苦挣扎，即便是业界规模较大的领先企业也难以帮助用户建立确实有效的安全防护能力。而在用户方面，由于在多年“狭隘”合规安全观的引导下，出现了“网络安全出不了大事，只要别被查就行”、“网络安全咋投入都不够，所以做到最低成本合规就行”的错误观念，不仅使政企机构的网络安全防护能力存在普遍短板，更反过来制约了网络安全市场的发展。

在眼前严峻的网络安全形势下，我们可能别无选择，只能在传统合规导向的基础上，进一步强调在对抗环境下提升网络安全防护的实际有效性，并加强落实网络安全责任，联合网络安全产业界有责任感、有能力的厂商共同向政企机构用户倡导正确的网络安全理念，从而打破用户在网络安全对抗性等方面的认知不对称，推动用户的觉醒并支持他们构建积极主动的网络安全防御体系。随着用户的觉醒以及对网络安全防护有效性的追求，网络安全市场的内需规模自然会持续扩大。

4. 安全立法和有效的网络治理是中国网络安全产业的重要保障

网络安全产业发展所需求的并非网络的乱象，当前需要检讨的是对严峻情况的麻木，而绝非应期待有更严重的事件来启迪对安全的认知。同时为网络安全创造宽松的研究环境和对黑产以及地下经济的纵容完全是两回事。安全产品可以防御攻击和恶意代码，但不可能作用于攻击者，后者是国家法律机器所要打击的对象。地下经济固然很难彻底消亡，但过度旺盛的地下产业会耗尽社会应对能力，同时带来不确定和非预知的风险，其

最终有可能导致用户彻底失去信心。而同时，恶化的安全形势，以及不断被黑产掌握和利用的 Cyberwar 级别的攻击手段，亦会进一步削弱通用产品的能力，而更进一步提升行业用户、大的互联网厂商自建篱笆和私人卫队的意愿，从而反过来进一步弱化安全行业。

因此网络安全产业的发展，恰恰不能只是黑暗丛林中的摸索，而同样需要安全立法和网络治理能力的有效提升。

四、产业应急之策

如果完整梳理中国网络安全产业的问题和症结，非本文篇幅所能覆盖，因为事实上很多问题，并不只是存在于一个行业，只是当这个行业显得特别弱小时，每一个障碍就都会显得那么明显。但换言之，可能每一个障碍的突破和释放，都可能让弱小而坚韧的产业带来新的生机。如近期国务院关于取消商用密码科研单位审批的决定，就是为安全行业释放的一个利好。

日前，政协委员、启明星辰公司严望佳女士提出了从用户角度“设立首席安全官制度”、从产业角度实现“供应链透明制度”、从新技术角度，加强电子政务云安全的提案。而亦有包括笔者在内的近 20 家安全厂商的负责人，联名上书，向国家建议“提高我国信息安全投入在信息化建设中的占比”、“取消最低价中标等”的建议，这些都是行业认识在求索、摸索中发出的呼喊。其中既有治本长略，也有应急之策。笔者希望把同仁这些好的建议再度陈列，这些正是产业救急之策。

- ●建立信息安全披露机制，遏制用户自欺、厂商欺人的现象。
- ●建立首席安全官制度，实现政企用户有人对安全负责。
- ●将合规安全观更新为博弈安全观，建立明确的应对威胁的导向。
- ●调整“内容安全”和网络安全的投入占比，有效盘活 Nexus。
- ●中止低价中标的游戏规则，释放反腐红利，让用户获得更可靠的服务，厂商获得合理回报。
- ●推动建立供应链透明制度，充分了解威胁分布，进一步尊重研发与创造。
- ●安全厂商抱团出海，在当前美国产业信誉受损的情况下，建立我们自己的市场体系。
- ●改善既有投入的有效性，让“老三样”发挥基础作用。
- ●对重点网络安全产业进行免个人收入所得税，提升人才招聘竞争力，降低其融资运作和结构调整成本。

当前完全可以选定网络安全产业，作为一些新政策的试点和新红利的特区。我们以业内联名建议取消低价中标的这一建议为例，其实是在反腐取得初步成效，一种不能腐、不敢腐的状态正在形成的情况下，让用户需求重新成为评价安全投标的主要依据。把反腐红利首先释放给网络安全产业。

五、尾声

两会已经结束，十三五的建设即将展开。“网络安全”一词在今年的政府工作报告中，鲜有提及，这会昭示一种新的导向么？有人解读，在经济下行的压力下，要避免过度考虑安全问题带给产业太多的束缚和羁绊。如果这种揣摩正确的话，这里我们亦能反映出安全行业所带来的角色尴尬，即其未能很好的履行为产业保驾护航的职能，反而从一定程度上在体制、管理和技术上给信息化进展带来了影响。

但毫无疑问的是，伴随着信息化的高歌猛进，网络安全的潜在市场空间正在全面拉大。但这这种机会亦需要中国的网络安全企业和从业者自身主动求变，寻找机遇。而非等待某一个或几个惨痛的事故、甚至再出一个斯诺登，来助推安全认知的达成。

中国崛起、大国博弈将带给那些真正的建设者和保卫者一个机遇，中国网络安全的从业者必将用双手先打破那个精致的小时代的幻想，再去投身一个属于我们的大时代。

（感谢杜跃进、潘柱廷、沈逸、赵粮、穆瑛、黄晟等业内同仁长期以来对本话题的共同讨论，本文从中吸取了大量营养。亦感谢我的同事 Billy、Angel 等对本文的贡献）