新 闻 动 态

标题新闻

奥巴马监控项目改进措施“收效甚微”

据路透社 2013 年 8 月报道，美国总统奥巴马限制美国政府全面监视项目的计划目前备受批评。针对由斯诺登引发的泄密事件，奥巴马称他决定采取四项措施：首先，他计划与国会合作，寻求对反恐怖主义的《美国爱国者法》进行适当修改；第二，与国会一起，寻求改革秘密的涉外情报监视法院，该法院的任务是审议执法机构针对个人搜集情报的要求。第三，公开更多关于国家安全局项目的细节，从而试图恢复斯诺登泄密案所破坏的民众信任；第四项措施是建议一个高级别外部专家组，来监管美国的监视项目。美国国家安全局拒绝对奥巴马的提议发表评论，尚不清楚国会是否接受这些提议。许多有影响力的议员坚决维护该监视项目，称其为发现恐怖主义威胁的重要手段。

美媒曝光情报机构黑色预算

据《纽约时报》9 月 2 日报道，《华盛顿邮报》8 月 31 日获取了斯诺登手中关于美国情报机构经费的 178 页文件。该文件总结了美国 16 个情报机构成功和失败的行动，这些情报机构的雇员总数达 107,035 人。这份文件显示，情报机关在截止于 9 月 30 日的财政年度中申请的预算为 526 亿美元，与 2011 年创纪录的 546 亿美元相比略有下降。在那之前的十年里，情报开支一直迅速增长。中情局在这些经费中占有最大份额，该局不仅执行由情报人员参与的传统间谍活动，还开展情报分析，现在也在针对巴基斯坦和也门的恐怖主义嫌疑人进行无人机空袭。几十年来，两党政府都将情报开支列入了通常称为“黑色预算”的分类，声称让对手了解美国在花什么钱会有损于美国的安全。从 2007 年开始，被称为“国家情报项目”的年度开支项目总金额才被公之于众。另外，每年单列的军事情报预算还有 230 亿美元。中情局申请的预算达到 147 亿美元，远远高于两大技术间谍机构。进行监听的美国国家安全局申请的预算有 108 亿美元，负责运行监控卫星的国家侦察局申请的预算则为 103 亿美元。

8 月美国智库涉华研究动态主要涉及亚太安全与海湾政策

综合美国媒体报道，2013 年 8 月中旬至月底，美国智库在涉华研究方面主要关注中美关系、亚太安全与中国在海湾地区政策等问题。

在伍德罗·威尔逊国际中心 8 月 27 日主办的“中国崛起为世界力量：对美国意味着什么”的研讨会上，与会者认为中国实力的持续增长会给美国带来挑战，但绝对不是一场新的冷战。

在美国战略与国际问题研究中心、台湾政策研究院及菲律宾战略与发展问题研究所举办的“2013 年度亚太安全论坛”研讨会上，与会者围绕亚太地区经济合作与冲突、美中日新领导层的改革前景、台湾的角色及策略、南海与东海争端等问题展开了小组讨论。

美国战略与国际问题研究中心 8 月在《海湾分析报告：中国在海湾地区的平衡举措》的分析报告中指出：在未来几年内，中国对海湾地区能源的依赖将日趋加大，而中国想要在该地区保持平衡则面临越来越大的挑战。

美国战略与国际问题研究中心高级研究员在 8 月一篇题为《日中海上互信建立与沟通机制》一文中认为，中日之间在过去 5 年里建立起的三大海上沟通机制除了取得一些原则性共识之外，并没能发挥太大实际效力。如果这些协议能够得到签署和有力执行，就会有助于在钓鱼岛争端加剧之际妥善管理双边海上活动。

美刊称中国的网络安全保护有待增强

据《华盛顿邮报》新闻网站 2013 年 9 月 4 日报道，美国情报机构前雇员斯诺登揭秘美曾对中国网络和手机用户发动黑客攻击之后，中方对自身易受攻击性的担心骤然增加。在中国，因特网用户越来越苦于自身的脆弱性。从很多方面来说，中国的网络安全问题比美国更为普遍，其用户受到的保护更少。目前，中国政府和网络安全部门正在推进一项国家战略，以保护计算机系统内的信息。业内分析人士说，中国目前对自产科技安全产品的需求大大增加，同时很多人呼吁禁止在政府和行业敏感部门使用美国生产的电脑硬件。许多业内分析人士相信，尽管中国为军方等部门储备了最好的防御性网络安全技术，但对于大多数中国人来说，每天都会因大量黑客攻击而遭受损失。中国政府委托进行的一项调查估计，60%的中国因特网用户个人信息曾在网上被窃取。去年进行的另一项学术研究估计，中国网络黑客造成的经济损失高达 8.52 亿美元。中国国内大量使用的不能及时更新漏洞补丁的盗版软件也是造成计算机系统脆弱的关键原因。

双汇收购美最大猪肉生产商交易获批

综合美国媒体 2013 年 9 月 8 日报道，双汇与史密斯菲尔德两家公司 6 日联合发布声明，称这宗收购交易已经获得由美国财政部牵头的外国在美投资审查委员会(CFIUS)的批准。此联合声明在史密斯菲尔德公司公布完一份财政报告数小时后发表。据悉，CFIUS 一直对外国企业收购美国公司且涉及科技、电信、国家安全领域时格外关注；而部分美国国会议员担心中国公司并购史密斯菲尔德可能会控制美国猪肉产业链条，并且影响美国的食品安全问题。史密斯菲尔德公司将于 9 月 24 日召开特别股东大会，就该交易进行投票。之后，此次交易活动将尽快结束。不过，部分投资者上周向史密斯菲尔德股东透露，届时他们计划投反对票，因为“感兴趣的买家”双汇实际上会以高于 34 元每股的价格进行购买，这可能成为完成此次交易的潜在障碍。全球规模最大的生猪生产商及猪肉供应商史密斯菲尔德今年 5 月 29 日宣布，已同意接受中国肉类加工商双汇国际控股有限公司的收购，收购金额约为 71 亿美元。双汇已承诺保留史密斯菲尔德现有的业务、员工及管理层。

朝鲜问题有助于巩固美中两国的牢固共识

据美国外交政策聚焦研究计划网站 2013 年 8 月报道，由于伊拉克和阿富汗逐渐淡出美国记忆，朝鲜作为对美国国家安全的最新威胁进入了美国的脑海。伴随着朝鲜发出的即将发动攻击的警告，许多外交政策分析人士认为朝鲜半岛的事态体现了中国和美国之间的必然对立。然而，我们必须要从宏观的角度看待国际体制的基本结构。中国在美国制裁朝鲜这一问题上的矛盾态度是否对范围更加广泛的国际秩序构成了挑战？如果没有，那么美国和中国之间这种假定的对立关系——至少在朝鲜问题上——或许没有什么意义。实际上，这并非典型意义上的对立。反过来，朝鲜需要汲取的真正教训是，中国政府并不愿迎来一场有可能升级的危机。在过去几个月里，中国并没有支持朝鲜的好斗行为。与之相反的是，中国与美国和韩国联手，进行了危机遏制，以此来应对导弹试射。中国已经表现出为“妥善处理有关问题做出不懈努力”的意愿。尽管美国威胁要加大在太平洋地区的军力，但美国国务卿约翰·克里也宣称，朝鲜危机是美中两国加强对话与合作、共同约束朝鲜的一个机遇。美国总统奥巴马满意地指出，中国正在“重新考虑”其对朝政策。中国不仅没有对美国的行动表现出敌意，反而公开表示愿意与美国进行合作。中国已经开始谨慎地参与为现有国际体系奠定基础的国际制度与机制，并承认其合法性。一直有这样一种观点认为：中国目前正在打造实力，以便在日后成为一个一流大国。中国在未来将采取行动，增强其在世界

上的相对实力。中国在非洲的活动以及该国扩大的军费极有可能继续阻止经济低迷的到来。这种举动并不意味着中国领导人希望对现有体制进行根本性的改变，中国目前的行动符合并且不违背世界秩序。

解密文件显示日本钓鱼岛气象站计划曾遭美国反对

综合外媒报道，2013 年 9 月 5 日解密的美国官方文件显示，1971 年日本计划在钓鱼岛附近修建气象站计划终因美国政府的反对而未能实施。报道称，美方的顾虑是担心日本的这一做法会导致地区局势的不稳定。据日期为 1971 年 1 月 11 日的美国驻日大使馆官方电报等记录显示，日本政府向美方传达了欲在钓鱼岛附近建立气象站的计划后，当时的美国国务卿罗杰斯以“会增加与台湾、大陆对立的风险”为由，指示美国驻日大使馆反对日本建造气象站。当时的驻日大使迈耶也表示担忧，认为这是日本试图在美国支持下加强主权主张的一种尝试。

重点关注

专家称先发制人是保护美国安全的最有效途径

编者按： 过去 70 年来，美国最仰仗的三个安全战略手段——威慑、预防和先发制人从未很好地发挥功效。在小型恐怖组织和黑客网络带来的“大规模破坏时代”，先发制人成为保障美国安全最后也是最大的希望，这类先发制人行动的优点在于其物质成本非常低。其挑战在于对越来越多信息的需求，因此世界各国应继续搜集和利用各种数据。

过去 70 年来，美国最仰仗的三个安全战略手段——威慑、预防和先发制人——从未很好地发挥功效。如今，由于符合文职决策者和军事战略家的思维定势和一些机构的利益，它们仍奄奄一息地维持着。当前，最为紧迫的事就是重新思考这些概念，甚至是抛弃与之相关的习惯做法。

在俄罗斯制造出自己的核武器后，美国对于预防性战争的热情冷却下来。因此，艾森豪威尔总统在 1954 年放弃了预防性战争，代之以威慑政策。大规模报复没有能阻挡过去半个多世纪以来盛行的叛乱风潮。托马斯·谢林在其军事著作《军备与影响》中对这一战略的总结是，大规模报复是“一种自提出以来就在走下坡路的学说”。

随着洲际弹道导弹的崛起和核弹头数量的快速增加，人们很快就明白了拥有这些武器的真正

价值就在于阻止他们的使用。但是战略学家和决策者们还是付出了巨大努力试图想出如何发动核战争，因此，直到冷战结束，战略威慑也仅在维持核和平方面发挥了作用，而世界各地在此期间发生了许多常规战争和非常规战争。

但这一切已经成为过去。自从进入新千年，开始与“基地”组织的长期冲突以来，人们又开始希望威慑、预防和先发制人的手段或许能够比过去更有用，鉴于敌人现在是一个网络而非国家，威慑的基本原则集中体现在拒绝而非惩罚方面。作为一个恐怖网络，它没有进行威胁的明确领土，因此焦点必须是“拒绝”让敌人达到目的。在某种程度上，美国本土防御措施已经取得了一点这样的威慑效果，但这并没有从整体上威慑恐怖主义，最近一批美国驻伊斯兰国家的使馆关闭正好再次证明了这一点。那预防性战争又如何？美国前总统布什曾用这一招发动了对伊拉克的入侵，但由于美国没有面临迫在眉睫的威胁，所以美国没有必要为之付出高昂的代价。

由于威慑概念已经奄奄一息，预防性战争信誉扫地，因此先发制人成为保障美国安全的最后也是最大的希望。尽管这一概念已经证明不适用于大规模杀伤性武器，但在小型恐怖组织和黑客网络所带来的“大规模破坏时代”，先发制人是我们迫切需要的。对一处恐怖分子藏身地或训练营的空袭，对黑客控制的恶意僵尸网络进行攻击，这些先发制人的手段可以减少外界对美国的威胁。

这类先发制人行动的优点在于，其物质成本非常低。其挑战在于对信息的需求，以便能够实施这些打击行动。由于先发制人需要以精确了解为基础，因此世界各国政府应当继续搜集和利用大数据，并逐渐看到这些情报系统的目的和意义。

（文章来源：2013 年 8 月美国《外交政策》杂志网站）

G20 峰会：美俄关系与中国

编者按：中美在 G20 峰会继续讨论双边问题的同时，中俄两国领导人也在峰会上举行密切会晤。与此同时，本次 G20 峰会也是一次美俄双方处理紧张局势的机会。虽然当前美俄之间的气氛紧张，作者认为两国之间的共同利益并不少，尽管在叙利亚问题上有分歧，但两国关系不至于弄僵。考虑到中美俄三国的复杂关系，美俄关系的发展也会对中国的外交走向产生影响。

中国想要美国承认中国正走向强国之列，不仅是在经济领域，而且在战略问题上。奥巴马总统可能在此次 G20 峰会间隙和习近平主席会晤，继续谈论有关朝鲜、网络安全、人权、气候变化、双边贸易及投资等问题。尽管目前美国推行亚洲重心战略，但奥巴马还是可能会考虑中国的想法。

在三个月前的加州会面之后，奥巴马表示两国摩擦不可避免。“但从过去四年我所了解的情况来看，两国人民都希望看到友好合作的双边关系。”奥巴马在某一场合表示。

除此之外，中国国家主席习近平还将和东道主、俄罗斯总统普京会谈。习近平将中俄关系描述为大国之间最友好的关系，并表示两国将世代友好，永不为敌。中国是俄罗斯武器的主要买家，今年 7 月两国在日本海举行了规模最大的海军联合演习。

本次峰会的一大热门议题无疑是叙利亚。中俄两国都坚决反对美国军事干预，尽管叙政府可能使用化学武器。两国都呼吁各方保持克制，通过政治途径解决问题——这让美国有些出乎意料。

叙利亚危机也加剧了美俄矛盾。普京拒绝承认美国情报部门认定叙总统阿萨德对民众使用化武。要知道中国是叙利亚最大的制成品进口国，而俄罗斯则提供叙政府军使用的大部分武器，并且是叙利亚最坚实的盟友。因此，本次 G20 峰会也是一次美俄双方处理紧张局势的机会，尤其是当叙利亚成为双方的主要分歧。

斯诺登事件之后，奥巴马取消了在 G20 峰会前和普京会晤。此时，美国很可能重蹈上世纪 90 年代处理对俄关系的覆辙。柏林墙倒塌后的十年里，华沙条约不复存在，苏联也已解体，但克里姆林宫仍然具备军事威慑的实力，甚至可以动用核武器，但所幸每当危机来临时，领导人都头脑清醒。当时的美国总统老布什和国务卿贝克着力促成美俄关系走向缓和，尽管戈尔巴乔夫和叶利钦都有些不太愿意。

但在接下来的几年里，美国的对俄政策不太明智，甚至有些极端，而俄罗斯也没有走好外交棋局。无疑，俄国的国力和影响力大不如前，外界把俄国看得无足轻重。俄罗斯反对北约军事干预塞尔维亚和科索沃，但却被晾在一旁；它在联合国投出的否决票，北约也没有当回事；它对美国入侵伊拉克提出警告，但无济于事。中俄曾联手反对在利比亚设立禁飞区，但结果却是该国易主，而联合国的法规却没有任何调整。

暂且不论美国及其盟友的做法是否合理，在俄罗斯看来，这些都是有针对性的。在上世纪 70 年代中期，绝对不可能发生这种事情。克林顿总统和小布什总统甚至连假装给俄罗斯面子的表示都没有，虽然这样做是出于实力优势的现实，但似乎并不明智。

过去的十年见证了数不清的分歧，通过峰会来寻求和解似乎不太可行（甚至连“峰会”一词都有些奇怪，尤其是当俄罗斯不再经常出现在峰会上）。美俄在许多国际问题上存在分歧，如叙利亚、伊拉克、科索沃、塞尔维亚等。另外，普京在国内开展反美运动，在电视台上进行反美宣传，控制言论和公民结社，监视宣扬自由的政治家及一些由美国资助的非政府组织，同时启用主张反美的官员。

后来斯诺登不请自来，美国要求将其引渡回国。奥巴马表示斯诺登必须被遣返，但普京不这么想。奥巴马取消和普京会面，因为已经没有友好的基础。确实是这样吗？即便如此，是否明智？和中国不同，俄罗斯对叙利亚展开多方面的援助，如物资、军事、经济等。虽然中国也在联合国框架内反对美国对叙动武，而且在南海上中国正在捍卫自己的权益，可能会和美国发生摩擦，但习近平主席仍然和奥巴马总统在加州举行了非正式会晤。

其实，美俄之间的共同利益并不少，尽管在叙利亚问题上有分歧，但两国关系不至于弄僵。两国都担心伊朗核问题，以及伊斯兰原教旨主义。俄罗斯支持美国提出的武器禁运，但将来却不一定。中东局势也是美俄关注所在，关于削减导弹和战略核武器的谈判也在进行之中。

此外，俄罗斯在一些重要领域支持美国，如当巴基斯坦境内通往阿富汗的道路被切断时，俄罗斯让北约军队从北部进入阿富汗。美国对普京的一些国内政策持不同态度，但这不适合在双边会晤时提出。国家领导之间的会谈主要是关于双边关系或共同关心的国际问题。本次 G20 峰会是俄罗斯展示实力、寻求合作及缓和与他国矛盾的一次机会，尽管形式大于内容。同意参加会晤虽然并不意味着能达成共识或取得成果，但其本身就说明了双方可以有转圜空间。人们常说，外交官一般和敌人谈判，而不是盟友。峰会上双边会晤的成本是很低的，可以出于尊重，尽管可能不是发自内心。

无疑，普京和奥巴马之间任何会晤的气氛会很紧张，这却符合美国的利益，能显示出美国的宽宏大度。但现在改变计划已经太晚，普京可能无法接受被怠慢。美俄关系还得往前走，但此次事件会让情况变得更加复杂。

如果将来两国元首会晤，议题应该是关于国家利益的。会晤不应被看成是美国对于俄罗斯的施舍。美国总统应从国家利益出发考虑是否和俄罗斯总统会晤，包括会晤的利与弊、两国合作的可能性、减少互相威胁等。无论两国关系能否转暖，美国应该认识到给予俄罗斯和前苏联同等的尊重一点都不难。要知道在冷战最高潮时，苏联的核武器更有威慑力，而今日的俄罗斯也不容小觑。考虑到中美俄三国的复杂关系，美俄关系的发展无疑也会对中国的外交走向产生重大影响。

（文章来源：2013 年 9 月《国家利益》网站　梁辰编译）

美国官员谈中美网络安全和相关政策制定

编者按：美国国务院网络问题协调官认为中美之间就网络安全问题会建立起更加牢固的关系，两国需要一个完整的法律架构或者全新的概念结构。随着近年来信息技术的快速发展，网络

安全在世界各国都受到越来越多的重视，欧盟和北约在鼓励成员合作、应对网络威胁以及防范网络战争问题上都采取了不同程度的举措。但是各国在网络安全方面的确存在一些差异，与不同国家商议双边协议的过程会有助于塑造各自国家的网络安全政策。

美国和中国正在讨论关于源自中国的恶意网络通讯有所增长的问题，这是奥巴马政府推动解决政策问题努力的一部分。随着网络安全融入平民和军队生活的几乎每一个方面，这些问题已经变得十分重要。

美国《防务新闻》刊登了对美国国务院网络问题协调官克里斯托弗·佩因特的一篇专访。佩因特曾是白宫负责网络安全政策的高级主管，他表示虽然有一些政策上的问题无法得到解决，但是努力加强合作和帮助定义网络攻击和网络入侵之间的区别才是最关键的。

在谈到中国网络工作小组取得的成绩方面，佩因特谈到奥巴马总统已经把他的担忧表达得十分明确，所以美国需要提出这些关切并建立一个持续的对话，而不只是每年把他们提一次。同时中美也需要在如何建立更好连接和网络透明的问题上持续对话，这样双方就可以找到方法来合作。举例来说，中美两国是否可以找到一种方式来应对第三方的威胁呢？这很重要。这样树立信任，也会使双方更加安全。随着时间的推移，这会帮助我们建立一个更加牢固的关系。在今年年底之前，中美还会有第二次会面，两国还会在闭会期间进行讨论。

关于爱德华·斯诺登泄密事件对网络安全对话的影响，佩因特认为很多国家之所以想讨论这些问题，是因为他们都意识到这些问题对他们自身的发展是多么重要。佩因特确实相信中美两国会继续在这方面展开很不错的对话。但是也不能盲目乐观，因为这确实存在很多挑战。

现行法律足够管理网络安全这个领域吗？还是需要其他条约或者协议来确立网络安全的道路规则呢？佩因特认为人们对网络安全有多半是错误的认识，认为它与现实世界完全不同。网络安全存在许多领域，包括潜在的网络安全冲突的领域，也适用我们在现实世界多年使用的规则，特别是像联合宪章和武装冲突法这样的规则。网络安全需要一个完整的法律框架或者一个全新的概念结构。尽管如此，在网络安全方面的确存在一些差异，在涉及多个利益攸关者的系统及管理方面存在一些问题。

目前各个国家如何处理网络安全政策问题呢？它会不会影响国际对话？十年之前这个问题还没有被任何国家列入政策议程。但是佩因特认为这个情况在美国已经发生了巨大的变化。网络安全办公室的设立，还有在白宫、国务院、国土安全部、司法部和商务部设立的协调员部分地证明了这一点。许多国家都正考虑这个问题，并且已经在他们的政府中提高了这个问

题的级别。作为世界上最大的区域一体化组织和军事组织，欧盟和北约在维护网络安全方面也有一些共性做法。

今年以来，欧盟继续加强在网络安全方面的制度和机构建设，不仅成立了网络安全犯罪中心，还积极推动了相关的立法工作。在具体实施过程中，欧盟的一个重要做法是提倡成员合作，要求所有成员共同确保数字环境安全，同时，成员国要和欧盟委员会共享早期风险预警信息。此外，欧盟还主张政府部门与私营部门之间的合作。对于网络威胁，欧盟初步将其分为三个层次。第一层次为网络事故；第二层次为各种形式的网络犯罪；第三层次为网络窃听和有关政府背景的网络攻击。

北约同样提倡成员国之间的合作。2010 年北约里斯本峰会通过了未来十年发展战略，正式将网络威胁作为北约面临的重大安全威胁之一。北约秘书长说保护自身网络安全对北约来说只是最基础的任务，下一步北约将考虑作为一个军事联盟如何应对网络安全。目前，北约对外宣称，在网络安全方面只是做好防御，并没有发展进攻性网络武器的计划。但实际上，北约近年来已经加强了在网络战争方面的研究。为了在有可能发生的网络战争中抢占主动权，欧盟提出了要发展网络安全方面的工业和技术，从而尽可能减少对国外技术和产品的依赖。

美国认为多数网络安全的行为适用于现行法律。在其他的国家、尤其是中国和俄罗斯的情况又如何呢？佩因特认为联合国专家政府组已经达成了一个重要的共识。这个组织包括了中国、俄罗斯、美国和英国这样的国家，总共有 15 个。他们在总结报告中提到一点：包括联合国宪章和武装冲突法在内的国际法适用于网络空间。对于怎样把这些国际法的概念应用到网络空间，各国还需要做很多工作。

在谈到美国如何通过网络安全对话完善问题时，美国总统已经宣布了与俄罗斯联邦建立双边信任的举措，这在整个网络安全领域开了先河。这是一个很好的透明的方法，可以合作来抵御来自第三方的威胁。在采取手段抵御僵尸网络，或者其它第三方的攻击和入侵问题时，美国已经做的一件事就是与国土安全部密切合作，因为他们经常通过他们的技术路径与美国接触，美国尝试了把这个与外交工作对接，在外交的层面上与他们的外交部或者其他级别的政府部门打交道。

目前存在的一个难点是要设法把第三方入侵和第三方攻击与其他一些违反国际安全的行为区分开来，建立清晰的分界线。世界上多个国家也在商讨双边协议。近年来随着信息技术的快速发展，网络安全在世界各国都受到了越来越多的重视。

（文章来源：综合外媒报道整理）

叙利亚问题会阻碍美国的亚洲再平衡战略吗？

编者按：美国的再平衡战略能够维持下去吗？ 随着美国干涉叙利亚问题将可能导致对美国战略分散的担忧，这一质疑会不可避免地继续下去。对此，美国分析界认为：干涉叙利亚问题是否影响美国亚太地区再平衡战略将取决于美国军事打击叙利亚的强度和持续时间。如果美国决定维持军事卷入叙利亚问题，政策制定者应明确阐明这将如何影响到美国在亚洲的行动和投入。

美国总统奥巴马决定向叙利亚反政府武装军提供轻武器和弹药反映出美国外交政策辩证法的基本事实。在本届政府以及整个华盛顿政治圈内，人道主义干涉是政策制定者和政治幕僚必然持有的默认立场。通过排除法找出奥巴马总统做出这一决定的背后逻辑就很容易看清上面提到的事实情况。或许，有人会认为总统觉得是时候扭转叙利亚问题的局势，使其有利于反政府力量而不利于阿萨德政体。

现实总是比理论更复杂，同样的道理也适用于外交和国家安全战略。因此，奥巴马政府 2011 年制定的重返亚太地区的重点战略和投资亚洲再平衡战略在实施的时候要比最初一系列演讲、文章和评论中提到的复杂得多。

自从美国的亚太政策宣布以来，来自亚太地区的美国盟国、合作伙伴以及来自潜在竞争对手国家的学者和政策制定者一直在问同一个问题：美国的再平衡战略能够维持下去吗？在国家安全顾问多尼伦、国家安全委员会亚洲事务高级主管巴德尔、国务卿希拉里·克林顿以及负责东亚和太平洋事务的助理国务卿坎贝尔相继卸任后，不断有人提出上述担忧，因为这些人被认为是再平衡战略的背后推动力量。当新任国务卿约翰·克里开始他的中东穿梭外交时，这样的担忧更加强烈，有些人担心克里的行动表明美国忽视了在亚洲的利益。

当然，颁布的政策并不仅仅体现了制定者的个性。美国政府人员中依然有大量的亚洲专家以及非常高效的政策制定者，他们致力于维持并深化亚洲再平衡战略。并且，重返亚太地区从根本上讲是总统的政策，奥巴马总统在第二任期间已经阐明了将继续保持对该地区的投入，维持地区贸易和外交活动的发展势头，在华盛顿接见亚洲六国领导人，并对泰国、缅甸和柬埔寨进行了国事访问，这也是奥巴马担任总统以来第五次访问亚太地区。

然而，有关再平衡战略的可持续性的质疑会不可避免地继续下去，并且美国干涉叙利亚问题将可能导致对美国战略分散的预想和担忧。尽管中国政府官方表态反对美国干涉叙利亚问题，但通过与中国学者的私下交流可以看出他们对美国的行为反响不一——有人对美国愿意卷入中东混乱表示惊讶，有人对美国出于何种利益干涉利比亚表示完全不解，还有人情不自禁地表现出希望看到未来美国卷入中东困境而不能脱身的场景。

在美国再次推动在中东采取军事行动（这一次的对象是叙利亚）之际，亚洲政府官员、外交家和分析人士不由质疑美国对于亚太地区到底有多投入。换句话说，“重心”是否还有意义？以及，它对几十年来依赖美国安全保证实现和平和繁荣的亚洲国家意味着什么？

美国有可能袭击叙利亚，这对奥巴马政府把重心向亚洲转移的外交政策将产生什么样的影响呢？美国安全中心的亚洲事务分析员帕特里克·克罗宁认为，美国在为可能对叙利亚发动攻击做准备之际，哈格尔照样出访与亚洲防长会晤，这对亚洲地区来说是一个重要的迹象。克罗宁说：“这些国家实际上都在看着美国，不仅仅是经济影响，最终还有安全保证。如果美国在这种会议上不露面，取消计划好的行程，这会释放一个完全错误的信号。”

然而，这对奥巴马政府把军事、外交和经济资源重心向亚洲地区转移的策略来说意味着什么呢？美国企业研究所的亚洲事务分析员迈克尔·奥斯林说：“叙利亚让奥巴马失去了他的亚洲势头。这不是因为叙利亚有那么重要，而是因为这集中体现了这样一个问题：我们说我们会选择地区，我们想离开某个地区然后把精力放到另一个地区，可是却做不到。”

重心转移亚洲所需的资源本应来自美国从伊拉克和阿富汗撤军节省的资源。不过，凯托研究所的亚洲事务分析员道格·班多说，即使在为叙利亚增兵之前，预算削减就已经减缓了部署进程。班多说：“我们现在在叙利亚看到的迹象显示，美国在资源减少的情况下维持这种全球存在是多么的困难。而这会影响一切的。”

现实情况是干涉叙利亚问题是否影响美国亚太地区再平衡战略将取决于美国军事打击叙利亚的强度和持续时间。截止到目前，美国的野心看起来相对有限。美国两艘航空母舰和五艘驱逐舰已经在该地区部署就位。美国似乎已经做好了打击叙利亚军事力量的准备，用最近媒体报道的话来说，目的就是“威慑、惩罚并降低”阿萨德政府的军事能力。值得注意的是部署在该地区的两艘航空母舰和五艘驱逐舰都不是从亚太地区转移过来。国防部长哈格尔最近对东南亚进行了重要的国事访问，并向媒体表示“尽管中东问题层出不穷，但该地区仍将是重塑国际事务的重要组成部分”。至少从目前来看，干涉叙利亚问题会牺牲一些高级政策制定者和军队领导人对亚洲政策的关注。不过，亚洲再平衡战略肯定能存续下来。

如果干预叙利亚问题程度加强或持续时间延长，亚洲再平衡战略将面临真正的考验。美国高层领导承诺会定期访问亚太地区，一旦延期或缺席，将给该地区传递美国外交重心可能转移的强烈信号。并且，高强度、长时间干预叙利亚问题将必然导致军事资源从亚太地区转移出来。这将给美国的盟友以及潜在的对手传递出一种已经遭受预算限制的美国军事力量将面临现实局限的强烈信号。

美国可以采取一些措施缓和亚洲地区对美国在该地区军事力量持续问题的担忧。首先，美国要努力向该地区的盟国和合作伙伴提供更多的军事援助，使这些国家有能力为包括地区稳定、海上安全以及人道主义援助行动在内的公共利益做出贡献。然而这不能解决全部问题——该地区依然需要美国的军事能力和领导力来维持地区稳定和繁荣，打造军事能力而不提供领导力只会导致军事竞赛、地区竞争并造成地区不稳定。

更加重要的是，美国现任领导人有责任诚实、明确地阐明美国在叙利亚问题以及亚太地区的承诺和目标以及不会为了其中一个而牺牲另一个。确实，美国决定避免长期军事卷入叙利亚问题是完全可以接受的，一方面是因为美国的资源和重心最好用于世界其他地方。如果美国决定维持军事卷入叙利亚问题，政策制定者应明确阐明这将如何影响到美国在亚洲的行动和投入。

学者和媒体仍会关注有关美国在亚洲地区承诺和保持军事存在的问题。确实，不管美国有多少军事设施和部队驻扎在亚洲地区，不管美国总统或内阁成员访问过多少次该地区，不管美国在该地区投入多少，签订了多少自由贸易协定，上面的问题会一直被提出。美国战略家和政策制定者的任务不是阻止这些问题，而是确保美国对世界地缘政治重心——亚洲地区的承诺能够在美国干涉其他地区并做出承诺的时候存续下来。在资源有限以及对美国军事力量需求多元化的时代，战略家必须能够分清轻重缓急。这是作为全球大国必须面对的现实，这也是对二十一世纪的战略家提出的要求。

（文章来源：2013 年 9 月《国家利益》网站，王子磊编译）

焦 点 分 析

美国国家安全局暗中开发强大信息解码技术

核心提示：最新披露的文件显示，美国国家安全局（NSA）在长期的加密技术战争中占了上风，它利用超级计算机、技术花招、法院指令和幕后劝说，对互联网时代保护日常通讯隐私的主要工具造成了损害。加密技术可以为国际商业和银行系统提供防卫、保护商业机密和医疗记录等

敏感数据，并自动为美国及世界各地民众的电子邮件、网页搜索、网络通讯和通话提供安全保证。上述文件表明，国家安全局绕开或破解了大部分加密技术。

NSA 会在信息被加密前潜入目标计算机获取相关信息。在一些案例中，公司表示，它们受到了政府胁迫，不得不交出自己的主密钥或是建立后门。此外，NSA 还利用自己作为世界上最有经验的密码制造者的影响力，秘密在世界各地的软硬件开发商所遵循的加密标准上设置了薄弱环节。“过去 10 年中，为了破解各种广泛使用的网络加密技术，NSA 针对多个方向大力开展工作”，2010 年的一份备忘录表示。“现在正在获得密码分析能力，此前被丢弃的海量加密网络数据目前可被利用。” 这份备忘录来自一场与 NSA 对应的英国机构政府通讯总部（简称 GCHQ）为员工举行的关于 NSA 成就的通报会。

最近几个月，斯诺登披露的文件显示，NSA 的行动范围甚广，从世界各地获取了大量通讯内容。而关于加密讯息的文件现在极其详细地讲述了 NSA 是如何确保自己能够解读搜集到的讯息。虽然 NSA 成功破解了加密技术所提供的很多隐私保护机制，但是这种成功并未改变如下规定，即禁止有关部门在没有得到授权的情况下，故意以美国人的电子邮件或电话为窃取目标。然而这份文件表明，隐私保护技术并不能完全限制 NSA 的行动。2011 年，一名联邦法官曾尖锐批评 NSA 违反了上述规定，并误导了外国情报监视法庭。按照 NSA 的规定，它可以在解密国内外任何加密讯息或分析其技术特征期间储存这些讯息，不论时间多长。

自 1952 年成立以来，NSA 就开始专攻解密技术，并把这项任务看作自身使命的基本要素。NSA 官员表示，倘若无法解密恐怖主义者、外国间谍以及其他敌人的讯息，美国就将面临巨大风险。就在最近几周，奥巴马政府向该情报机构了解了基地组织领导人关于一次恐怖主义行动的通讯内容以及叙利亚官员关于发生在大马士革外围地区的化学武器袭击的讯息。NSA 官员表示，如果此类通讯信息能够用无法破解的加密技术进行隐藏，NSA 就将无法开展工作。但有些专家表示，NSA 绕开及削弱通讯安全保障的做法或许会带来严重的意外结果。他们说，NSA 正在与自己的其他重大使命（除窃听以外）——保证美国的通讯安全——背道而驰。

NSA 力度最强的一些工作都集中在美国广泛使用的加密术上，其中包括安全套层（Secure Sockets Layer，简称 SSL）、虚拟专用网（virtual private networks，简称 VPN），以及 4G 智能手机所使用的保护措施。曾联合设计 SSL 协议的著名编码师保罗·科克回忆称，NSA 在 20 世纪 90 年代曾要求在所有加密系统里安插叫做“Clipper 芯片”的政府后门，并最终失败。“但他们不顾一切，还是这么做了，而且没有告诉任何人，”科克说。他说他理解 NSA 的使命，但是他担心允许 NSA 不受限制地获取私人讯息会带来危险。“情报界一直都在担心世界会陷入永远‘静默’的

状态，但他们如今却不费吹灰之力就能在瞬间全面侵入人们的隐私之中，”他说，“这简直是间谍活动的黄金时代。”

这些文件属于《卫报》向《纽约时报》与非营利性新闻机构分享的逾 5 万份文件之列。它们主要侧重 GCHQ ，但其中有数千份文件来自 NSA 或跟它有关。这些文件显示，该机构仍然没有攻克所有的加密阻碍，正如斯诺登 6 月在《卫报》网站上进行网络问答时所提到的。“正确使用强大的加密系统，是少数你可以依靠的手段之一，”他说。不过他也告诫道，NSA 经常会完全绕过加密系统，方法是针对一端或者另一端的计算机，在文本被加密之前或者解密之后获取它们。该文件明确指出，NSA 认为自己解密信息的能力非常重要，并在就此与中国、俄罗斯和其他国家的情报机构开展竞争。

NSA 成立之初，加密还是一种鲜为人知的技术，主要供外交官和军官使用。过去的 20 年里，随着互联网的兴起，它已经变得无处不在。即使新手也知道，如果电脑屏幕上的网址旁边出现一个小小的挂锁图案，他们的信息交换就被自动加密了。NSA 机密文件明确表示，由于严格加密之后的效果非常好，该机构的成功有赖于跟互联网公司的合作——要么获得它们的自愿合作，要么用法庭命令迫使它们合作，或者暗中窃取它们的加密密钥，又或者修改它们的软硬件。

知情人士告诉《纽约时报》：有一次，在美国政府了解到某外国情报目标订购了新的计算机硬件之后，美国制造商同意在硬件出货之前植入一个后门。NSA 在其 2013 年的预算申请中强调了“与各大电信运营商保持合作伙伴关系，使全球网络有利于其他信息搜集活动”——也就是说，获得更多的窃听机会。据《卫报》报道，NSA 跟微软公司的管理层合作，可以在加密前访问该公司人气最高的服务项目，比如 Outlook 电子邮件、互联网通话与聊天软件 Skype，以及该公司的云存储服务。微软强调，自己只是遵从了政府的“合法要求”，而且在某些情况下，合作显然是迫不得已的。熟悉内情的人士透露，政府曾经要求一些公司交出所有用户通信的加密密钥。如果公司高管拒绝执行秘密法庭颁发的这个命令，可能会被处以罚款或监禁。

NSA 的文件显示，该机构有一个名为密钥供应服务(Key Provisioning Service)的内部数据库，里面是特定商业产品的加密密钥，可以自动解码很多信息。如果解码所需的密钥不在数据库中，它会向密钥收回服务发送请求。后者就会设法获取相应的密钥。如何得到密钥是保密的，但一些独立的密码专家称，许多密钥很可能都是通过秘密侵入相关企业存储密钥的计算机服务器来获取的。与此同时，NSA 也刻意削弱了开发人员采用的国际加密标准。该机构 2013 年的预算申请中阐述的目标之一是“影响商用公钥技术的政策、标准和规范”，而这种技术是最常见的加密方法。

密码专家早就怀疑 NSA 在一个标准中植入了漏洞。这个标准于 2006 年被负责美国加密标准

的国家标准与技术研究院所采用，后来又被拥有 163 个成员国的国际标准化组织采纳。NSA 的数份机密备忘录似乎证实了，微软的两个密码破译人员 2007 年在标准中发现的致命漏洞是该机构的手笔。NSA 编制了这个标准，花大力气把它推向国际社会，并在私下里称这个任务是“需要精妙应对的挑战”。“最终， NSA 成为了唯一的编撰者。”备忘录中写道。

即使某些看似旨在保护美国人通信的 NSA 项目，有时也被用来削弱这种保护。举例来说，NSA 旗下的商业解决方案中心曾以改善美国网络安全为名，邀请加密技术开发机构来展示它们的产品和服务。但一份绝密 NSA 文件显示，该机构的黑客部门使用同一个项目培养并“利用跟特定行业合作伙伴之间的敏感合作关系”，以达到把漏洞植入到互联网安全产品中的目的。

通过引入此类后门，NSA 悄无声息地获得了在公开场合未能取得的成效。20 年前，美国官方对一些强大加密软件的流行担忧起来，比如程序开发员菲尔 •齐默尔曼设计的“完美隐私软件”。如果推行下去，NSA 将始终掌握密钥，实际上会使电子加密失去作用。

这项提议在很大范围内遭遇了强烈反对，并出人意料地团结了一批人，其中包括参议院里的政治对头，比如来自密苏里州的共和党人约翰 • 阿什克罗夫特和来自马萨诸塞州的民主党人约翰 • 克里，还有电视传教士帕特 • 罗伯森、一批硅谷高管，以及美国公民自由联盟。

一份 NSA 文件显示，到了 2006 年，通过破解保护性的 VPN，该局已攻破了三家外国航空公司、一个旅行预订系统、一个外国政府的核能部门，以及另一个外国政府互联网服务的通讯系统。到了 2010 年，英国反制加密的计划已成功破解了 30 个目标的 VPN，而且设立了再破解 300 个的目标。不过，这些机构的目的是要摆脱逐个破解目标工具的局面，迈向实时解译通过全世界光纤和互联网交换机的所有信息，仅需事后搜寻解密材料来获取有价值的情报。2010 年的一份材料呼吁，采取“全新的方式来进行随机解码，而非逐个破解目标”。就在当年，一份报告文件宣称，NSA 已获取了针对加密网络聊天与电话的“突破性能力”。该机构在破解 SSL 和 VPN 上也不断有所斩获。不过，NSA 担心，一旦解码的“实情”广为人知，就会丧失长时间努力得来的优势。GCHQ 概述计划的一份文件中警告，“这些能力是项目中最为脆弱的部分，无意间泄露这一简单‘实情’的话，可能会让对手警觉，并导致能力的迅速丧失。”

自从斯诺登的揭秘激起外界对 NSA 触角太广、侵犯隐私的批评，美国科技企业就面临着消费者和公众的审视。一些人认为，业界与政府的关系太过紧密。作为回应，一些企业开始反击他们眼中的政府的霸道行为。谷歌、雅虎、微软都施加了压力，希望允许它们披露有关政府下达秘密合作要求的更多信息。由于不愿满足 NSA 的要求，小型邮件加密企业干脆关门，因为公司认为 NSA 要求的是机密客户信息。另一家企业宁可终止邮件服务也不愿满足类似的要求。

实际上，当 NSA 不断得寸进尺的时候，业界都做出了让步。Lavabit 的创始人拉达尔·莱韦森给失望的客户写了一封公开信，给出了不详的警告。“除非国会采取行动，或是法院做出强有力的判例，”文中写道，“我强烈建议，任何人都不要把自己的私人信息交给与美国有任何实际联系的公司。”

（文章来源：9 月 6 日《纽约时报》）

本刊编者注：本刊所载文章的观点不代表本刊主编的观点，仅供读者参考