CBN 智库
Research Institute
第一财经研究院

Committed to Improving Economic Policy.

Research Note

2015.09.28. (CBNRI RN15-059)

（编译）马鑫 / 研究员 maxin@yicai.com

www.cbnri.org

研究简报 中国与世界

网络威胁与中国：美国的政策难题

作者：加力·克莱德·霍夫鲍尔（Gary Clyde Hufbauer）,系彼得森国际经济研究所高级研究员

来源：美国彼得森国际经济研究所中国经济观察：http://blogs.piie.com/china/?p=4514，2015 年 9 月 22 日

2015 年 8 月，在习近平主席访美前夕，白宫线报暗示美国将制裁源自中国的商业网络间谍行为。但这一警告在两周后又被撤回。本周会面时，两国总统定会讨论包括商业网络间谍在内的网络威胁问题。而作为谈话成果的反映，美国将可能调整未来的报复措施。

即使在美国立场看，元首谈话仍不令人满意。解决网络威胁问题带来了多重政策难题：

1、区分网络战，军事网络间谍行为及商业网络间谍行为；

2、识别犯罪者；

3、计划恰当的应对措施；

中方十分清楚这三个难题，而这一认知会深刻影响奥巴马与习近平的谈话方向。在评论这些难题前，首先总结一下商业网络间谍行为的各方面情况或许能有所裨益。

一、商业网络间谍活动的结果与损失

贸易秘密通常通过两种途径获得：昂贵的搜索和开发，长年的实践经验。相反的，商业网络间谍行为可以通过快捷、低廉的方式获取商业机密。如果没有有效的强制措施和严厉的处罚制止，网络间谍行为就意味着通往制造和分配技术前沿的巨大捷径。

商业网络间谍的主要目标是开发创新技术的公司。根据网络安全公司 Fire Eye 的报告，中国黑客攻击的美国公司涉及电子、电讯、机器人技术、数据服务、制药、移动电话服务、卫星通讯和图像及商业应用软件等领域。这些产业恰好也是中国战略性新兴产业倡议中提到的重点领域，是中国十二五计划的一部分。

据战略与国际问题研究中心的报告估计，由网络间谍和网络犯罪带来的总体经济损失约达每年一千亿美元。这一数据包括了利润、

出口和就业的损失。据美国商业部估计，2014 年间，美国每 10 亿元出口额支持了 5796 个就业岗位。尽管由网络间谍行为造成的美国出口损失总量仍然未知，但创新技术产业的失业量高达成千上万。

二、区分不同类型威胁

中美双方或能就网络战的大致范围达成共识，并可能宣布“不首先使用”政策。这或许会是此次元首访问的一个显著成果。应用网络恶意软件摧毁电网、电讯、互联网或者银行系统是网络战的典型案例。而在这些挑衅之外，还有存在相当大的难以定义的灰色地带。如何看待攻击如亚马逊这种某一大公司网站的行为，或是给如花旗银行这种某一大银行制造网上混乱的行为？如果两国元首能就网络战的大致范围达成共识，即可成立一个中美工作小组着手研究这类细节。这将成为两国元首会面的一个积极成果。

奥巴马总统上周表示，军事网络间谍行为是当代治国战略的一大重点。可能的中国网络攻击就属于这个范畴，它或将危及美国人事管理处约 2200 万份文件。据前 CIA 主管 Michael Hayden 观察，在此情况下，美国国家安全机构（NSA）也将设法弄到其外国对手的人事记录。然而，由于军事网络间谍行为相当普遍，且美国在此领域也有相当的技术，中国的军事间谍行动并不需要针对性回应。

然而军事和商业网络间谍行为之间的区分并非总是那么明确。中美双方应该会认同网络窃取亚马逊或阿里巴巴的商业机密属于商业间谍行为。但是，意图窃取中国移动公司或是德国电信公司的商业机密的网络间谍行为到底属于军事还是商业性质？双方或许在这一问题上难以达成共识。

一个更大困难在于，两国能否达成共识，政府应避免与商业间谍行为的联系。在美国看来，政府还应致力于起诉所有形式的商业间谍活动。而中国或许持不同观点。正如很多国家一样，美国立法禁止其领土内通过网络或其他途径采取的一切商业间谍行为。基于 1996 年经济间谍法案，已有大量犯罪起诉案件得到受理。中国可能也有类似的法规，但少有实施行动见报。

三、识别犯罪者

熟练的电脑黑客都会隐藏自己。而在实施经济制裁，或者进行黑客反击之前，美国需要充分确定其识别了正确的目标对象。但在这种背景下，“充分”意味着多大程度的确定？百分之九十，九十五还是九十九？而美国又是否准备好了公开它确定目标对象的证据？

2014 年，针对索尼公司出品的一部名为 Interview 的电影的网络攻击成为了关注焦点。黑客威胁将轰炸未取消放映这部电影的影院。美国情报官员称，朝鲜与此次事件有关。2015 年 1 月，奥巴马签署行政命令，对朝鲜政府部门及 10 名政府官员实施制裁。对于朝鲜的指控看上去十分合理，因为这个低级喜剧电影的主角就是金正恩。然而，相关的技术证据却从未公开。

同时，尽管表明了对于中国网络间谍活动的密切关注，美国政府也从未公布相关证据，将此类活动联系到明确的中国政府机构、公司或个人。如果奥巴马决定要在中美元首会面后实施针对性制裁，美国需要公布其确定这一目标的技术依据。

四、计划有效应对措施

作为自发回应，美国联邦调查局于 2015 年 7 月 23 日发起了警觉经济间谍行为的全国性活动，提醒美国公司防备危及商业机密的网络间谍行为。这一活动源于 2014 年间激增的相关事件。据报道，网络间谍事件的数量同比

2013 年增长 53%，而中国为主要犯罪来源。有五名中国官员因此受到起诉，但他们都得以在中国国内确保安全，此后可能也不会面临美国法庭审讯。

2015 年 4 月 1 日，奥巴马签署了 13694 号行政命令，声明网络威胁成为全国性的紧急事态，并会“冻结某些从事重大恶劣网络活动的个人的财产”。这就为美国应对网络攻击奠定了法律基础。基于这条行政命令，美国可以对威胁到国家安全或经济的黑客实施制裁。其中规定的相关活动包括攻击关键性基础设施，扰乱电脑网络，窃取个人资产、商业机密或个人信息用于商业用途。而借助美国司法的有力支持，被发现参与到网络战中的个人与实体的资产将可以被冻结，通过这类银行账户的商业交易也可以被禁止。

13694 号行政命令并未提到黑客反击。这就意味着美国政府仍可能采取此种形式的报复措施，或者默许由美国公司实施的“反黑”回应。

五、习近平访美之后

对于可识别犯罪者的商业网络间谍活动，13694 号行政命令为强有力的经济应对措施奠定了法律基础。奥巴马并未承诺美国不会进行黑客反击。事实上，在最近一次商业圆桌会议的讲话中，他强调美国政府“正在准备一系列措施，提醒中国我们不仅仅是有些恼怒。如果这个问题不解决，将深刻影响到中美双边关系，而我们也将采取一些对抗性措施以引起中方重视。”在习近平访问之后，此类间谍活动是否会大幅减少还有待观察。如果没有，美国会公开识别犯罪者的证据，并全力实施法定制裁吗？还是会在特殊情况下实施黑客反击？让我们拭目以待。CBNRI