

美国如此针对华为，到底在怕什么？

•  冈特·舒赫 战略管理咨询公司 Debrouillage 创始人

2019-04-15 07:27:10 来源：观察者网

https://www.guancha.cn/GunterSchoech/2019_04_15_497646_s.shtml

【文/ 观察者网专栏作者 冈特·舒赫，译/杨瑞赓】

美国非常清楚自己为什么害怕华为，因为各种通过技术刺探情报的事他们统统做过。我们所面临的变化，不是谁不想再开展间谍工作，而是掌握技术优势的人变了。

美国的虚伪从它的措辞可见一斑，这种清晰划分敌我的世界观还真是“令人欣慰”。

如果“我们美国”使用间谍手段，我们称之为“情报”或“侦察”，“保护国家利益和国家安全”的做法当然都是“正当合理”的。

如果“他们中国”这样做，我们称之为“间谍”、“网络攻击”、“渗透”、“犯罪”、“侵略”，当然这是“不道德的非法行为”等等。

既然华为创始人任正非曾是一名解放军军人，那么这便是其从事间谍活动的准证据，虽然在美国，拥有军队背景也同样大大有助于一个人从事社会和政治活动。



2019年1月18日，中国深圳，华为董事长兼首席执行官任正非在华为总部接受日本媒体的采访。

图片来源：东方 IC

让我们把话说开了吧，任何理性思考的人都知道，世界各个国家和各国领导人都在互相刺探情报，不仅出于军事和政治目的，也是为了经济利益。

孙子在兵法中高度强调间谍的重要性；东罗马帝国派间谍假扮成僧侣到中国窃取蚕桑丝绸技术的秘密；我的祖国德国 19 世纪时派工程师去英国窃取炼钢技术……诸如此类的事情数不胜数。

如今，华为已经被全世界各大媒体泼上了“间谍”的脏水。尽管许多人还是第一次听到华为这个名字，却已经把它与“间谍”这个词牢牢联系在一起。

为什么美国要花这么大力气来打击一家公司？

从美国1月29日对华为的刑事起诉来看，其所指控的行为最早可以追溯到2007年。为什么要等这么久？也许在那个时候，美国是欢迎低价产品的，并不将华为视作技术威胁。

现在，美国担心中国未来会像美国对待别国那样对待美国：几十年来，美国一直在监视监听盟友和敌人，从而获取政治、军事和经济利益。

如果你以“华为”与“商业间谍”进行检索，就会发现除了那种胡乱预测未来的文章外，多数是美国国家安全局渗透华为设备的案例。

在“狙击巨人（shotgiant）”行动中，美国国家安全局侵入了华为总部服务器，不仅拦截电子邮件，还窃取了源代码——对任何科技公司而言，源代码都是王冠上的宝石。

2014年，华为发言人比尔·普卢默评论道：“这件事如果属实，那么具有讽刺意味的是，他们对我们所做的事，恰恰是他们一直指控中国政府通过华为所做的事。”

现在，针对孟晚舟和华为的诉状都把华为内部邮件作为证据，美国是如何获取华为内部电子邮件的？这是一种巧合吗？

唯一有“实锤”的指控也引用了被截获的电子邮件。

一名华为雇员在2017年被判有罪，因为他窃取了德国电信的美国子公司T-Mobile开发的名为“Tappy”的机器人手臂的相关机密。这款产品可以自动点击智能手机屏幕。

尽管它牵涉到的是4G设备的屏幕，而不是5G网络组件，可这件事仍然作为“各种商业间谍活动”的证据被大书特书。不过，作为“受害者”的德国电信却仍然在继续采购华为的手机和网络。

你若以为美国只通过庞大的监控网络监听东欧敌对国家，从不窃听德国政治或商业机密，那未免也太天真了。位于巴伐利亚州巴特艾布灵的监听中心成立于1947年，一直受美国国家安全局领导，直到本世纪初因为监听德国的行动激起公愤才将管理权逐渐移交给德国联邦情报局。美国对德国采取的手段包括监听移动和固定电话，监控互联网信息，以及拦截卫星传播信号。

作为全球监控网络“梯队系统”的一部分，巴特艾布灵监听中心是除英国和美国本土之外最大的监听站。

斯诺登曝光的文件揭示了美国是如何在互联网时代开展监控行动的。

《纽约时报》写道：“斯诺登文件还表明，美国国家安全局有另一个目标：更好地吃透华为的技术，寻找潜在的后门。”这样一来，当华为向美国的敌人出售设备时，美国国家安全局便能够针对这些国家的计算机和电话网络进行监控，并在必要时发起网络攻击行动。”

美国政府为了证明它想要表达的政治观点，会定期公布它靠网络入侵手段获取的信息。人们往往只注意到信息本身多么惊悚，而忽视了美国获取消息的方式。

以2019年2月8日的《纽约时报》为例：

“在2017年的一次谈话中，沙特王储穆罕默德·本·萨勒曼告诉一名高级助手，如果贾马尔·卡舒吉不返回沙特王国，且不停止对沙特政府的批评，他将赏对方‘一颗子弹’。卡舒吉已于去年10月被杀……”

为了提高可信度，消息提供者表示：

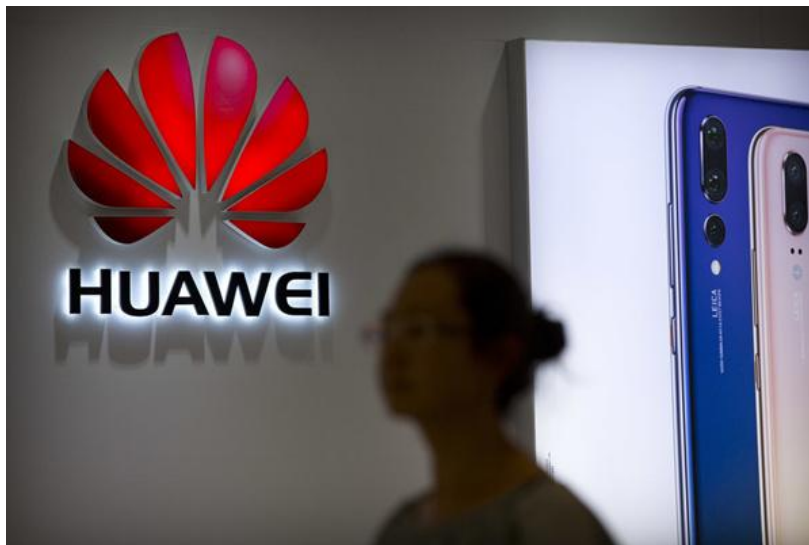
“……根据美国情报机构截获的谈话，这是迄今为止最详细的证据，表明在沙特特工将卡舒吉勒死于沙特驻伊斯坦布尔领馆并用骨锯将其肢解之前，沙特王储就早就考虑杀死卡舒吉了。”

如果我们能让受害者被骨锯肢解的惨状暂时离开我们的脑海，便会发现美国情报机构拦截了一个主权国家元首的电话，而且这个国家居然还是美国的盟友。

我们当然可以合理地假设，华为的技术跟诺基亚或爱立信一样，都存在被滥用的可能，而且某些情况下它们也确实遭到了滥用。

例如，2013 年有新闻曝光美国国家安全局和英国政府通信总部拥有苹果、黑莓和安卓手机用户数据的访问权，可以读取智能手机的几乎所有信息，包括短信、位置、电子邮件和笔记。

唯一的区别是，中国的利益相关方能更多接触到中国技术公司的信息，而西方的利益相关方能更多接触到西方技术公司的信息，但这只是相对的，不是绝对的。



2018 年 12 月 6 日消息，因怀疑违反美国对伊朗的贸易制裁，华为首席财务官孟晚舟被加拿大政府逮捕。图为 2018 年 7 月 4 日，中国北京，华为商店。图片来源：东方 IC

当苹果公司引入强加密技术时，2015 年和 2016 年法律诉讼接踵而至，美国政府根据 1789 年的《所有令状法案(All Writs Act)》，在至少 12 项法院命令中要求获取访问权限。在某些情况下政府给出的理由是应对恐怖袭击，另一些理由则是诸如信用卡欺诈等小事。在所有情况下，美国政府都要求苹果公司从锁定的 iPhone 中提取联系人、照片以及通话等数据。

现在想象一下，美国政府想向华为或中兴施压，要求它们编写代码来破解它们提供给客户的加密程序。

如果因为中国法律要求私企在某些情况下与情报和执法部门合作，就将华为排除在美国市场之外的话，那么根据《所有令状法案》，思科也应被排除在美国之外。

那么，美国禁止公务员使用华为产品和服务，以及强烈“鼓励”网络运营商不再售卖华为设备（比如强迫 AT&T 和 Verizon 在推出华为新款手机前夕突然放弃与华为合作），真的是怕华为通过手机监控美国公民吗？

看起来，这项措施更像是为了方便美国当局在必要时破解其国内流通的各种手机。

我是个现实主义者，非常厌恶任何形式的极端主义，无论是宗教的、政治的还是意识形态的。我可以接受这样一种现实，即双方都不是完全诚实的，都致力于维护己方利益，当然表面上还是会装装样子。

但如果有人决定要大举占领道德制高点，他本身需要经得起道德检验。

让我们剥开美国冠冕堂皇的道德说辞，那不过是为了愚弄那些容易哄骗的民众和盟友。

还记得震网病毒（Stuxnet）吗？

这是一种于 2010 年被发现的计算机蠕虫病毒。它的攻击目标是广泛应用于工业过程控制的监控和数据采集系统（SCADA）和可编程逻辑控制器（PLC）。震网病毒被认为是美国和以色列伊朗核计划而联合研制的网络武器。

震网病毒破坏了伊朗的 PLC，导致浓缩铀离心机异常加速自行毁坏。

此次华为事件可以说是当年卡巴斯基争议的翻本。俄罗斯软件制造商卡巴斯基的产品被认为是世界最好的杀毒软件之一。

自 2015 年以来，西方媒体指控卡巴斯基与俄罗斯政府关系密切，最后美国政府也做此表态。2017 年，特朗普签署法案，禁止美国政府和公共机构的计算机使用卡巴斯基软件。

从 2010 年左右开始，卡巴斯基软件暴露了一系列由政府资助的网络间谍和破坏活动。据《连线》杂志报道，“其中许多行动似乎是由美国及其盟友英国、以色列等国发起的。卡巴斯基尤其以揭露震网病毒而闻名。”

很难相信这一系列事件都是巧合。

因此，如果美国政府够坦诚的话，它应该这样说：“我们就是看不得华为成功，尽管它的成功理所应当，因为它使我们的情报和反情报工作变得更困难。因此为了掐断它的渠道，公平也好不公平也罢，我们各种手段都要用。”

（观察者网杨瑞赓译）