多普勒效应助力定位MH370航班

据美国有线电视新闻网3月25日报道，24日马来西亚总理纳吉布有关“马航失联客机MH370终结于南印度洋海域”的言论，开启了一个新的问题，即如何通过数字运算来确认这件波音777客机的航迹？

现在，我们可以确信“它不可能飞向北路”，英国卫星运营商国际海事卫星组织(Inmarsat PLC)执行副总裁克里斯·麦克朗林(Chris McLaughlin)这样表示。

马来西亚总理纳吉布24日表示，失联客机最后被追踪到的位置位于南印度洋中部海域，澳大利亚城市珀斯以西。而失联客机乘客家属告诉美国有线电视新闻网称，马来西亚航空公司此前告知他们，“机上所有人员全部遇难”。

24日的结论则再为已迷云笼罩超过两周的客机失联事件带来新的疑问。同时，也引发了要求让所有航班都被不间断追踪到的呼声。

麦克朗林将英国卫星运营商国际海事卫星组织以及英国航空安全事故调查局在确认最终航路时，所采取的以数学为基础的分析方法形容为“开创性的”。

“我们开创了一些新的东西”，他这样表示。

简言之，这个分析的过程是这样的：英国卫星运营商国际海事卫星组织的官员和工程师通过卫星信号的扩张或压缩，以决定失联客机究竟是飞离还是飞向卫星所在位置。

而扩张和压缩的含义是什么呢？你可能听说过多普勒效应(Doppler effect)。

“如果你坐在火车站里，然后你听到火车的汽笛声——而音高会随着火车的移动而发生变化。这就是我们所掌握的”，曾研究过多普勒效应的美国有线电视新闻网气象学者迈尔斯(Chad Myers)这样表示，“他们运用多普勒效应来研究客机所发送的脉冲信号，或者也可称为与卫星的电子通讯握手。他们通过飞机距离卫星所处64.5度的纬度位置的远近，来获知在十亿分之一秒单位下，信号是被压缩，还是扩张了。

每一次电子通讯“握手”都被用于分析它飞行的方向，迈尔斯这样表示。而麦克朗林则表示，这一新的算法，也经过了来自太空总署专家的同行评议，以及波音公司的支持。

运用这种分析方式更确切的确定飞机坠落地点是有可能的，迈尔斯表示，“运用三角法，工程师可以找到航班的角度。”

专家表示，他们对于飞机沿着南部航向飞行的信息并无意外。这一方向是上周卫星数据所揭示的两条可能航路中的一条。而北部飞向巴基斯坦的航路则布满雷达监控。巴基斯坦此前已经表示，他们并未在其雷达系统上发现MH370的踪迹。

麦克朗林表示，在可能的北部飞行路径上，未观察到着火或者失事的迹象，是难以令人置信的。

另据新浪军事3月26日报道，美国海军用于搜索马航MH370航班黑匣子的专用设备，将抵达澳大利亚，然后装载在海军舰艇上进行搜索行动。

那么，美国海军此次都出动了什么专用装备？

1、被动搜索——TPL-25拖拽搜索器

黑匣子在落入海中后，会自动以27.5K赫兹的频段发射声波信号。而TLP-25则是美国海军专用的黑匣子搜索器。

TPL-25搜索器长76厘米，宽约88厘米，重量约31公斤。该系统相比于美国海军的专用拖拽反潜声纳要迷你很多。

从性能上看，TPL-25可搜索6000米深度的目标，接收音频范围为3千赫兹到50千赫兹，拖拽航速为1-5节。

2、主动搜索——Bluefin-21无人潜水艇

相对于TPL-25的被动接收信号，此次美国海军携带的BlueFin-21无人潜水艇则是以主动搜索为主。

按照厂方数据，Bluefin-21总体造型和尺寸和一发533mm口径鱼雷类似——直径53里面，长4.93米，总重750公斤。与只能拖拽的TPL-25不同，Bluefin-21采用锂电池驱动，可以3节的航速巡航25个小时，最大潜水4500米。

Bluefin-21装备有一台120/410K赫兹主动声纳，用于海底扫描，搜索MH370客机在水下的碎片。需要注意的是，Bluefin-21的改进型Bluefin-21BP，装备有更强大的455K赫兹主动声纳，可以在距离75米和150米左右距离上，进行快速声纳成像。

综合中国新闻网
新浪网 2014.3.26

公安部:打击伪基站犯罪要从源头整治

“伪基站犯罪是近两年来迅速发展蔓延的一种新型违法犯罪，它可以强制截获手机信息，任意冒用号码，随意发送垃圾短信或诈骗信息，迷惑性强，潜在危害十分巨大。这也是群众对伪基站违法犯罪行为感受比较深的两点。”公安部刑事侦查局局长刘安成25日接受《法制日报》记者采访时这样评价伪基站犯罪的危害。

记者了解到，伪基站生产、销售、使用犯罪从2012年起以个案形式在各地逐渐呈现。针对这一新型犯罪，公安机关秉承早发现早打击的原则，两年来，公安部已组织全国公安机关开展两次专案打击行动，取得了一定成效。这次9部门联合打击整治行动开始时，公安部梳理出几千条重点线索，下发各地侦查，从设备研发生产等违法犯罪源头到产供销的违法犯罪网络进行全链条打击，捣毁生产窝点24处，打掉犯罪团伙314个，抓获嫌疑人1530名，缴获伪基站设备2600余套，取得比前两次打击行动更好的战果。

“目前打击伪基站违法犯罪活动也存在发现难、取证难的问题。”刘安成解释道，随着伪基站技术的不断发展，设备体积越来越小，可以放在汽车上而不被察觉。伪基站一般是在地下窝点秘密生产的，联系销售走网络和物流，并且使用假姓名、假联系方式、假银行卡，给取证带来困难。

刘安成说，伪基站违法犯罪的对象是不特定的。有的群众认为只是受到骚扰，不会去报案。受害人往往都是流动性的，这些都给公安机关调查带来一定困难。

《法制日报》2014.3.26

无人机能像鸟群一样协调飞行

一个匈牙利研究小组开发出一种无人驾驶直升机，群体飞行时就像一群鸟，能协调配合在空中形成队列、变换阵型，甚至追随一个“首领”，而这一切都无需中央控制系统。研究人员近日带了10个飞行器到布达佩斯郊外试飞，实地观察了它们的空中飞行效果。

这些飞行器由匈牙利罗兰大学物理学家达马斯·维塞克领导的研究小组开发。它们都有4个轮子，研究人员称之为“四脚直升机”，利用来自全球定位系统(GPS)接收器的信号导航，通过无线电来沟通彼此的位置，并计算出自己将要怎么飞。

据维塞克介绍，通常的无人机都设计为单飞模式。虽然此前也有其他小组研制过群飞机，但那些实验采取了一些捷径，比如只让直升机在室内试飞，或通过中央计算机来控制。唯一真正的自主无人机群是瑞士洛桑联邦理工学院机器人研究专家达里奥·弗洛里诺在2011年研发的，但他的飞机是固定式机翼，只能以固定速度飞行，而且不同飞机要在不同高度飞行以避免碰撞。“它看起来像一个群体，但并非真正的群体，因为它们彼此之间不能互动。”

相比之下，维塞克小组的无人机可以协调自身，排成旋转的环形或直线形。如果“告诉”它们前面有一堵墙，而墙中间有个缺口，它们还能排着队从缺口中挤过去。

据自然网站日前报道，他们的灵感来自于一款名为“Boids”的计算机程序，是加利福尼亚大学圣克鲁兹分校计算机图形专家克雷格·雷诺德在1986年开发的。雷诺德按照3个规则来设计虚拟飞行物的运动：配合邻居的平均方向、飞向它们、保持距离避免拥挤。这些规则包括对齐方式、吸引、排斥，能让计算机模拟鸟群飞行。此外，研究小组还解决了GPS信号噪音和延迟的问题，无人机群才终于成功。

“这是一项非凡的成果。”美国普林斯顿大学集体动物行为研究专家莱恩·科辛说，“这是第一次在户外演示利用仿生规则开发的恢复性动态集群。这也意味着，我们在实现大型协调性机群方面，将比许多人预期的要快得多。”

维塞克和研究小组已经向明年9月将在美国芝加哥召开的“国际智能机器人与系统大会”提交了他们的论文。

目前，无人机之间靠无线电通讯，有时会导致信号拥挤，给它们装上摄像机可能会解决这一问题。“鸟类都有极佳的视力，这不是偶然。”维塞克说，“下一大步是让直升机能互相‘看得见’。”

《科技日报》2014.3.26 文/常丽君

美安全局曾监控中国前国家领导人

美国针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。这是美国国家安全局前雇员爱德华·斯诺登提供的文件所表明的。

美国情报机构攻击的目标包括中国前国家主席胡锦涛、商务部、外交部、银行和电信公司。

美国国安局尤其花大力气监控全球第二大通信设备供应商华为公司。2009年初，该局启动了一项针对华为的大规模行动。华为被视为美国思科公司最大的竞争对手之一。美国国安局的一个特别小组成功渗透进了华为公司的计算机网络，并复制了超过1400个客户的资料和工程师使用的内部培训文件。

根据美国国安局的一份秘密文件，该局人员不但窃取了华为的电子邮件存档，还获得了个别华为产品的源代码，源代码被视为信息技术企业最神圣的东西。美国国安局渗入华为的深圳总部，因为该公司通过总部处理每个员工的邮件往来，所以美国人从2009年1月起就读取了该公司很大一部分员工的电子邮件—包括总裁任正非和董事长孙亚芳的邮件。

美国国安局的一份内部文件说：“我们获取了如此之多的数据，以至于我们不知道如何处理它们。”该局给出的监控原因是，“我们的很多目标是通过华为产品进行通信的”。此外，美方还担心“中国利用华为遍布世界各地的设施搞间谍活动”。不过目前仍不清楚，美国情报人员是否已经找到了这方面的证据。

该行动是在白宫情报协调员、中央情报局和联邦调查局的介入下实施的。

美国情报部门说，如果了解了该公司如何运行，那么未来将会得到回报。迄今为止，网络结构由西方主宰，但中国人将努力使西方的公司变得“更不重要”。那样的话，迄今由美国公司主导的互联网技术标准将被打破，中国将逐步控制网络中的信息流。

华为公司在美国的一位高管威廉·普卢默在一份声明中批评了这种攻击。他说，如果美国国安局真的实施了这样的行动，“现在应该知道，我们的公司是独立的，与任何政府都没有特殊关系”。

长期以来，美国官员一直将中国电信巨头华为公司视为安全威胁，竭力阻挠该公司在美国达成商业协议，担心它会在自己的设备中植入“后门”以便让中国军方或北京支持的黑客窃取企业和政府机密。

不过，机密文件表明，国家安全局正直接向华为的网络植入自己的“后门”。

国安局前雇员斯诺登提供的文件显示，该局窥探了华为位于中国深圳总部的服务器，获取了重要信息。

2010年的一份文件称，这项代号为“射中巨头”行动的目标之一是寻找华为和中国人民解放军之间的联系。但这项计划有了进一步行动：对华为的技术加以利用，这样当该公司将设备卖给其他国家—包括盟友和避免购买美国产品的国家时，国安局可以进行监视，如果总统下令的话，还能进行网络攻击。

国安局的这份文件说：“我们的许多目标通过华为的产品进行通信。”该文件还说：“我们想要确保自己知道如何利用这些产品获取进入(世界各地)我们感兴趣的网络的机会。”

美国官员一再说，国安局侵入国外网络只是为了实现合法的国家安全目标。国家安全委员会发言人凯特琳·海登说：“我们没有把搜集到的情报交给美国公司，以增强它们的国际竞争力或提高它们的利润。”但这并不意味着美国政府没有带着不同的目标开展自己的企业间谍活动。

华为在美国的一位高管威廉·普卢默说，华为不知道自己成为美国国安局的目标，“讽刺的是，他们对我们所做的恰恰是他们一直指控中国方面通过我们所做的”。

新华网 2014.3.24