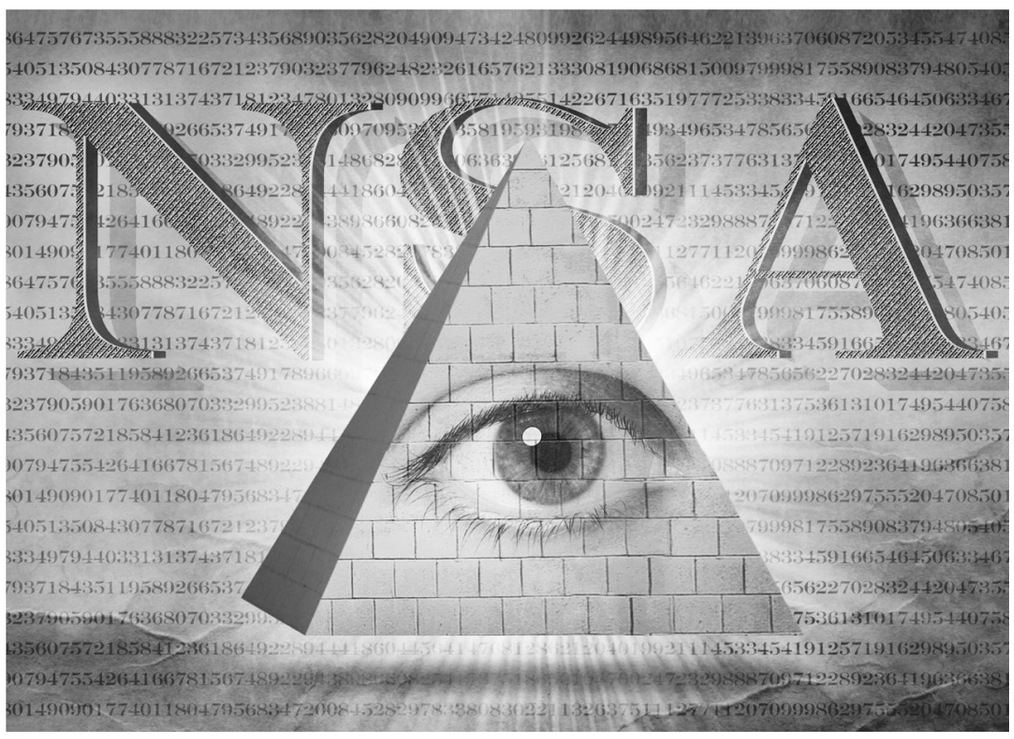

图片来源：WILLIAM DUKE

隐私的终结　信任的幻灭

斯诺登事件后美国数学家开始质疑与国家安全局的长期纽带关系

每年，美国国家安全局（NSA）的招聘者据说是全美数学家的最大雇主，该机构每年都会遍访联邦各大高校搜罗新人才。过去，它推出的职位非常“畅销”。“他们抛出的一个诱人点是，你整天都会解决复杂而有趣的谜题。”一位要求匿名的数学家说。他补充道，在 2001 年“9·11”恐怖袭击之后，“如果我可以利用自己的所学采取任何方式以杜绝类似事情再现，在道德上我都有义务去这么做”。过去十年，他曾多次丢下大学的研究事业，为该机构工作。

然而，随后由于意识到一些数学家的道德意识被蒙蔽，该机构的招聘变得复杂化。2013 年，NSA 原雇员爱德华·斯诺登发布文件揭露该机构一直在大规模截获普通美国公民的电子邮件和电话记录，而且 NSA 还可能有意破解全球普遍使用的保护个人电脑的数学标准。

此次事件动摇了这位匿名数学家的信念。“对于那些持有和我一样想法的人来说，NSA 任务的伦理性至关重要。”此次事件在数学界搅起一池浊水，让很多人质疑其与间谍机构长期的共生关系，该机构在学校培养数学家种子、支持相关研究、拨款经费并为数学家提供参与间谍行动的机会。

近日刚卸任美国数学学会（AMS）理事长的麻省理工学院数学家 David Vogan 一直督促该学会重新思考与 NSA 长期的紧密联系，但他却并未赢得学会其他官员的支持。

尽管如此，难以说服很多有天赋的数学家与计算机学家再为该机构工作的一个标志是，NSA 主任 Michael Rogers 不得不亲赴现场做说客。“你们很多人都是未来我希望竞争到的对象。”去年 11 月，他向斯坦福大学的听众说，“我们面临的最大挑战……是在当前的环境下让大家加入我们。”一名学生问他 NSA 会给“已对美国政府不再抱有任何幻想”的研究人员提供什么。Rogers 给出的回答有些牵强，他列举了“服务国家”与“做一些其他地方不能合法做的事情”的机会。

用经费缔结学术纽带

“NSA 需要数学家，就像造纸商需要树木一样。”Vogan 说。该机构雇佣了多少数学家很难证实，但其整体员工就达到上万人，其官方职责是为保护美国信息设计密码逻辑系统，同时利用外国信息系统的弱点，这些都要严重依赖数学。自 NSA 在 1952 年成立起，该机构就致力于数学军备竞赛，那些需要更加复杂的密码生成与破译技术。正如 NSA 一直承认的那样，它在维持美国数学界健康发展方面有着既得利益。

和该组织的其他活动一样，NSA 与数学界的绝大多数交往内容都属于机密。“我们不会发布项目特别预算。”该机构公共事务官员在给《科学》的电子邮件回函中说。即便是国会为该机构提供的年度总预算也属于涉密信息；据估计，相关拨款在 80 亿 ~250 亿美元之间。

每年 NSA 的财政预算仅有为数不多的项目公开，这仅是因为其涉及到由 AMS 进行同行评议的拨款项目。该机构今年将通过其数学科学项目投资 400 万美元用于研究拨款、研究生夏季实习、给大学教授学术休假让他们到该机构工作以及数学会议等。Vogan 表示，尽管与数学家每年从其他联邦机构收到的 4 亿多美元相比，这只是九牛一毛，但是对于为数不多的几个受益领域，如数论和概率来说，“这并非小数字”。

NSA 支持的科研项目的成果已见诸学术期刊。“他们希望通过论文使拨款得到认同。”波士顿东北大学的 Egon Schulte 说，他在组合数学方面的研究受到 NSA 拨款支持。这让直接追踪由 NSA 支持的学术产出变成可行。《科学》用谷歌学术搜索引擎对相关学术论文索引进行的一项分析显示，由 NSA 支持的研究产出自冷战和苏联解体以来稳步增长，仅在 1999~2012 年间略有减少，随后自“9·11”恐怖主义袭击后直线增长。仅 2013 年就有超过 500 篇文章表示受到 NSA 支持。

但是对于个人研究人员的直接拨款仅是 NSA 对数学提供的支持的极小部分。该机构共享给《科学》的资料描述了所支持的广泛学术项目类型，从学校 STEM（科学、技术、工程与数学）教育到大学实验室研究等。NSA 专家还会进行班级授课并评论科学事宜。还有一部分竞争性拨款项目用来支持科学夏令营、高中数学俱乐部以及计算机实验室。

这些拓展项目让该机构从一开始就与那些最有潜力的数学苗子建立了密切的联系。“你与学生接触得越早，你雇佣他们的机会就越大。”NSA 原人力资源部主任 Harvey Davis 在 2002 年的一次听证会上对国会说。Davis 还指出该机构一直与高等教育机构之间保持着张弛有度的和睦关系。“我们与大学制定决策的重要教授以及全国数学界都有密切联系。”他说。

在由 NSA 评定为“卓越学术中心”的 55 所高校，均有一名 NSA“代表”在该校担任全职。据《科学》搜集到的资料，他们发挥着该机构“影响研究与研究伙伴关系，决定网络世界与未来人才队伍的”的“门户”作用。NSA 的目标高校包括知名私立大学如普林斯顿大学、纽约大学、卡耐基梅隆大学，以及很多公立高校如北卡罗来纳州立大学、宾夕法尼亚州立大学以及加州大学戴维斯分校等。

粉碎信任的“恩主”

然而，该机构与高校之间的亲密关系近期却引发了一些争议。宾夕法尼亚州匹兹堡大学数学家 Thomas Hales 嘲讽说：“每个人都认识在 NSA 工作的校友，他们在该机构工作过一段时间后就好像得了健忘症，几乎没有例外，但没人关心这些。”但一些科学家了解到该机构在如何利用他们的工作之后，局面在 2013 年发生了转变。

在斯诺登事件之后，多数媒体的视线都转移到了 NSA 大规模获取美国公民的私人数据上。但对于 Hales 和其他很多数学家来说，该事件背后涉及更加隐晦的问题：他们看到的是对于现代互联网安全中心的攻击。

例如，当你在线核对银行账户时，这些信息会被银行服务器和你的个人电脑生成的一系列大数据编码。计算机会利用数学算法生成随机数字，尽管这些数字并非完全不能预测，但测量它们却几乎超越了全世界所有的计算能力。只要这些伪随机数据处于保密状态，加密后的信息就可以安全地通过网络，防止窃听者——包括 NSA。

但是该机构似乎打开了加密交流的后门。常规上，美国和国外的计算机行业都要采用由国家标准技术局（NIST）认可的安全标准，但是 2006 年 NIST 把批准印章加盖在了一个匿名数字生成器上（DUAL_EC_DRBG），并引发了错误。2007 年，微软公司计算机安全专家首先发现这个潜在错误，但事情却没有引起多少人关注。直到 NSA 内部备忘录被斯诺登公开，才揭露了 NSA 是这个错误算术的始作俑者。

“由 NSA 设计的这个算术有着明确的数学结构，可以万无一失地给他们打开一扇后门。”Hales 在一封于 2014 年 2 月由 AMS 发表的公开信中写道。他介绍说，自从那时起，“我的结论就被其他信源逐步证实”。比如，2014 年 7 月 NIST 的一份报告表示，NIST 只是在根据该情报局的命令行事。“NSA 在椭圆曲线领域极为优越的专业知识让 NIST 决定听从该算式。”该报告说。数学界的研究人员也表示，如果目标计算机使用的是 NSA 设计的其他安全产品，这一错误就更容易被利用。NIST 去年 4 月放弃支持这一错误标准，而 NSA 对此未作任何公开声明。

一些人在为该机构辩护。在 AMS 在线期刊发表的一封公开信《美国数学学会通知函》中，Richard George 表示他本人曾为 NSA 工作了 41 年，并表示他的 NSA 同事“绝不会做梦想去侵犯美国公民的权利”，尽管“任何团队中都会有几个‘烂苹果’”。对于 NSA 开启通向个人电脑的后门一事，George 写道：“我从未听说过任何与 NSA 相关的已被证实的缺陷；只是有些人含沙射影的传言。”

在《通知函》中，斯诺登事件激发了关于数学学会是否应该切断与该机构纽带的尖锐讨论。伊利诺伊州芝加哥大学数学家 Alexander Beilinson 也参与了激辩，他争论称，数学学会应该彻底与 NSA 分道扬镳。他表示，对公民的监控和软件的篡改似乎让美国成为一个“我年轻时期所看到的膨胀的前苏联”。数学学会理事长 Vogan 也对此极为愤怒。“NSA 可能还故意破坏商业加密软件。”他说，“我认为这种行为与医学研究领域为了追逐利益而造假别无二致；这样一项错误行动会永久地损害科学在全球的地位。”

尽管批评声音极多，该学会至今却未采取任何行动。Vogan 表示，去年 AMS 委员会针对此次事件的态度“非常可怕”，学会就 NSA 的道德进行公开声明一事没有表现出任何兴趣。他补充说，普通 AMS 会员大多也都抱有同样态度。截至目前，美国数学家也不愿脱离他们有些阴暗的、但却提供稳定经费支持的“恩主”。　（冯丽妃）

> “这种行为与医学研究领域为了追逐利益而造假别无二致：这样一项错误行动会永久地损害科学在全球的地位。

自动驾驶时代近在咫尺

未来 10 年内或将出现完全无人驾驶汽车

今年夏天，人们将能乘坐无人驾驶的电动班车，穿梭在英国格林尼治的大街小巷。这个耗资 800 万英镑（约合 1200 万美元）的项目是英国政府资助的无人驾驶汽车大科学项目的一部分，而它仅仅是众多追求交通运输革命的其中一项努力。降低交通事故死亡率在一定程度上刺激了无人驾驶汽车的发展——约 90%的事故是由司机失误造成的。这场竞赛致力于将汽车操控权从人转移到电脑，因为后者从不在开车时打瞌睡、看短信和喝酒。

几乎所有的汽车大型制造商都致力于开发某些自动化技术。而且，公众出人意料的热烈响应也刺激了汽车制造商和政府研究机构加速在这一领域的前进步伐。“我从未见过有什么能如此快地从概念变为产品。”美国交通部自动化高速公路研究项目负责人、汽车技术顾问 Richard Bishop 说。尽管仍然存在许多技术挑战，但开发者表示，他们能看到解决大部分问题的明确途径。

例如，在互联网巨头谷歌公司，迄今为止大部分无人驾驶汽车都采用了安装有全球定位系统接收器和绘图技术的标准载客汽车，还有些车辆安装了雷达以探测障碍物，激光测距系统来扫描周围环境，以及能鉴定红绿灯、建筑物标识、行人和其他车辆的摄影机。一台处理能力相当于数台台式机的车载电脑，将把所有信息进行结合，并确定车辆在既定情况下应如何驾驶。为了减少负载的驾驶算法，谷歌还在无人驾驶汽车上装配了极为精确的地图。

但怀疑者指出，这种地图设备可能将汽车限制在那些已经勘察得十分精确的地方，例如谷歌总部——美国山景城。但创建谷歌汽车项目的工程师 Sebastian Thrun 表示，扩展这些地图可能相对容易，这将作为该公司为谷歌地图拍摄全世界路况信息努力的一部分。

Thrun 表示，一个更困难的问题是，教会汽车如何响应所谓的“不可能事件的长尾巴”。他提到，在早期，谷歌团队开发出能处理十字路口和湿滑路面等频发的显著挑战的新算法。但当车辆行驶了数千公里后，他们记录了许多古怪事件，例如塑料袋飞过高速公路或一张长沙发被扔在道路中间。“一开始，有很多事情超出我们的想象。”Thrun 说。而处理这些稀少事件的唯一方法是，当事件发生时记录下来，在高性能机器学习算法的帮助下找出应答方案，然后模拟测试这些解决方案，并进行更多的驾驶训练。

Thrun 说：“如果我们做得充足，希望这个软件能与人类驾驶者一样安全”，甚至更安全。但这需要多长时间仍然是个开放性问题。谷歌公布的预计时间为 5 年，但该公司目前仍拒绝接受有关该项目的采访。

额外的安全性将来自车辆配备的类似无线网络的车对车（V2V）无线电设备，以帮助它们彼此发出危险情况警告，例如有车辆闯红灯。这将给予无人驾驶和有人驾驶汽车足够的时间相互避让。

图片来源：Pascal Goetgheluck

尽管 V2V 技术或许能成为无人驾驶汽车的一部分，但它的研发主要基于独立研究。这一概念作为欧盟道路安全项目的一部分已经进入实地测试阶段。测试中，许多汽车一辆接一辆跟在一辆卡车后面，就像鸭子妈妈身后跟着一群小鸭子。由于 V2V 信号能让每辆车都在卡车停下的瞬间同时刹车，因此能够避免追尾事故的发生。而且，由于流体动力学因素，这列车队至少能节省 10%的燃料。

此类实验引起了汽车生产商通用公司的兴趣。去年 9 月，该公司宣布将在未来支持 V2V 技术的发展。起初，这些汽车将几乎没有其他车辆进行交流。但美国国家公路交通安全管理局正计划发布新条例，要求在这十年的后期阶段，该国所有新车辆全部安装 V2V 无线电设备。

“这些车辆将仅广播最基本的安全信息：位置、速度和行驶方向。”佩络通技术公司总经理 Josh Switkes 说。该公司致力于重型卡车 V2V 技术的商业化。但他表示，这已经足以减少事故的发生，而且还能产生能源效益。不仅如此，通过车辆的协调行动还将拥堵降低至最小化，也能带来可观的燃料效率。如果汽车能够智能地询问红绿灯——车对基础设施系统（V2I），以调整自己适应道路车辆密度，将能减少停止时间。

最终，这些技术部署的时间表将依赖于更广泛问题的答案。这些汽车的费用是多少？谁能拥有它们——个人还是服务公司？当无人驾驶汽车发生事故时，责任方是谁？人们是否将信任它们？不过，鉴于今天创新的步伐，经验正在快速积累。　（张章）

科学线人

全球科技政策新闻与解析

美国国家同步辐射光源二期工程正式运行

美国能源部秘书长 Ernest Moniz（右）参观国家同步辐射光源二期工程。
图片来源：布鲁克黑文国家实验室

当地时间 2 月 6 日，在位于纽约厄普顿的美国能源部（DOE）下属布鲁克黑文国家实验室，前景看起来一片光明。能源部秘书长 Ernest Moniz 主持了实验室新的国家同步辐射光源 II（NSLS-II）正式运行仪式。此项工程耗资 9.12 亿美元，将成为美国并在一定能量范围内成为全球最亮的同步辐射光源。

“在 NSLS-II 开展的研究将探寻新型物质的基本结构，帮助推动低成本低碳能源技术的发展，促进环境科学领域的进步，并刺激医学突破的产生。”Moniz 表示。

NSLS-II 将产生非常密集的 X 射线、紫外光和红外光束，使包括生物学家、化学家和环境学家在内的研究人员在纳米级别上探测物质，同时以接近 10 纳米的分辨率分析物质性质。科学家将利用该装置在最小尺度上研究高温超导体、下一代硅片和生物蛋白。NSLS-II 产生的光束亮度将是其“前任”——已运行了超过 30 年的国家同步辐射光源的一万倍。

去年 10 月，NSLS-II 开始调试，然后逐渐加大力度至全速运行。研究人员将利用此装置的 7 条可用光束线开展第一批研究，但工程技术人员计划在接下来的 5 年里增加另外 25 条光束线。尽管 NSLS-II 的建设和它的最初光束线均由 DOE 的基础能源科学项目资助，但对于其他光束线的资助将来自其他机构，包括 DOE 的生物和环境研究项目、美国国立卫生研究院以及国家标准技术局。当建设工作全部完成时，该装置将拥有 70 条光束线，每年支持 4000 余名研究人员开展工作。

NSLS-II 主任 John Hill 介绍说，来自该大型装置的初始数据看上去非常令人期待。“这是一台绝妙的机器。看到自己的辛苦付出有了回报，人们都非常激动。”　（徐徐）

日本基金会“挑战”被忽视传染病

疟疾是日本一家新成立基金会攻克的目标疾病之一。
图片来源：U.S. Army Africa/Flickr

一家日本基金会将发起“大挑战”项目，努力探寻诊治被忽视传染疾病的创新方法。

全球卫生技术创新基金（GHIT）此前宣布，将为每位候选人投资 100 万美元用于“全新和改良药物、疫苗或诊断技术早期阶段的开发，以预防和治疗在发展中国家肆虐的传染疾病”。

上述挑战项目模仿并同比尔与梅琳达·盖茨基金会的“探索大挑战”项目合作，后者支持探索那些旨在解决全球卫生发展问题的高风险、高回报方法。

不过，GHIT 的挑战项目有一些独特之处。申请者必须是日本和非日本机构的合作人员。“如果你观察一下目前‘探索大挑战’项目资助金的组合情况，便会发现真的没有多少出自日本。”GHIT 执行董事 BT Slingsby 表示。该基金还将新发起的挑战项目视作对现有努力的扩展，目前它正利用日本的资源和能力，支持针对被忽视疾病的潜在药物的临床前和临床研发工作。新的“大挑战”将迎难而上，支持一些前景不错的药物在早期阶段的开发。这些药物可能最终进入 GHIT 资助更为慷慨的开发系统。

“大挑战”还将具有选择性，每年挑选 2 个、3 个或 4 个项目进行大约为期两年的资助，并希望这些项目随后能为药物开发的下一步作好准备。Slingsby 表示，他们期望每年提供 200 万美元左右的资助，而这对于他们正在寻找的早期想法已经足矣。

GHIT 成立于 2013 年 4 月，由日本政府、6 家大型日本制药公司和盖茨基金会共同支持。其目标是攻克疟疾、肺结核、美洲锥虫病、内脏利什曼病和其他折磨发展中国家贫穷人群的疾病。

Slingsby 介绍说，他们的“大挑战”项目将与盖茨基金会和其他致力于被忽视疾病的组织合作，“以确保我们在日本寻找到最具创新的药物，并保证我们的工作不只是简单的重复”。

申请自即日起已经开放，第一轮获胜者将在今年 8 月公布。　（徐徐）