NSA 网络战士如何帮助美国赢得（可以这样说）伊拉克战争

非官方中文译本 • 安天实验室 译注

文档信息			
原文名称	How NSA’s Cyber Warriors Helped Win (Sorta) The Last War in Iraq		
原文作者	Shane Harris	**原文发布日期**	2014 年 11 月 9 日
作者简介	Shane Harris（谢恩•哈里斯）是一位广受赞誉的作家和记者，撰写了大量有关情报和国家安全的文章。他的新书《网络战争：军事互联网复合体的兴起》探索了美国的新型网络战争的前线。 http://shaneharris.com/		
原文发布单位	《每日野兽》		
原文出处	http://www.matthewaid.com/post/102178369761/how-nsas-cyber-warriors-helped-win-sorta-the-last		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为		

	不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

NSA 网络战士如何帮助美国赢得（可以这样说）伊拉克战争

Shane Harris

《每日野兽》

2014 年 11 月 9 日

在其新书《网络战争：军事互联网复合体的兴起》的一部分中，《每日野兽》记者 Shane Harris 展示了 NSA 如何与伊拉克的军事伙伴合作，并永远地改变了战争格局。

Bob Stasio 从来没有打算成为一名网络战士。高中毕业之后，他就读于布法罗大学，进入了后备军官训练队项目。他的专业是数学物理，研究令人费解的量子力学和偏微分方程理论。在这所大学中，渴望毕业的学生沉浸在自然科学中，疏忽了核心课程所要求的一些主要科目，包括英语。在整个大学生涯中，Stasio 从来没有写过论文。

2004 年，Stasio 来到了华盛顿的刘易斯堡，当时他 22 岁。他的旅情报官看了一眼该少尉（Stasio）的简历，看到了其数学和物理学的背景，就告诉他："你去信号情报排吧"。

SIGINT（信号情报）指的是捕获和分析电子通信。正如情报学的任何分支一样，它是科学与艺术的融合，但是偏重于科学。该旅情报官曾在 NSA（美国国家安全局）工作过，知道 Stasio 的物理知识能够派上用场，因为大部分 SIGINT 涉及无线电信号、光纤传输和互联网数据包的技术收集。

Stasio 被分配到一个斯特瑞克旅，这是一个能够迅速行动的武装部队，能在短短几天中部署作战。Stasio 的任务是通过追踪通信信号来定位战场上的敌人，监听指挥官给部队下达的命令来洞察敌方意图，或监听排长从后方下达的空袭指令。Stasio 被编入第二步兵师第四旅"奇兵"，并被部署到伊拉克。他将与一组语言学家合作，这些语言学家是必不可少的，因为 Stasio 并不懂阿拉伯语。

Stasio 于 2007 年 4 月抵达伊拉克，成为了美国军队新"增兵"的一员。他可能会想他们是不是来得太晚了。Stasio 和他的研究小组看到美军受到叛乱分子、路边炸弹和迫击炮的无情攻击；伊拉克在不断升级的内战中濒临崩溃。外国作战人员从邻国叙利亚和伊朗不断涌入，而伊拉克被称为基地组织（后来演变成 ISIS）的恐怖分子网则对美国和联军、伊拉克政

府和伊拉克的什叶派发起了残酷的攻击。该恐怖组织的目的是打倒羽翼未丰的神权独裁统治的政府。

但是 Stasio 拥有叛乱分子没有的武器：存储着 NSA 监听站收集的电子通信和信号的服务器。在他被部署到伊拉克之前，Stasio 花了一些时间来研究叛乱分子：他们不遵循传统军事的垂直结构，那么又是如何形成一个网络的？Stasio 认为，如果他能挖掘到伊拉克的信号情报，包括叛乱分子的通话、电子邮件和短信，他就可以拼凑出他们的通信记录，或许能够由此了解其网络的规模和结构。Stasio 是 HBO 电视剧《火线》的粉丝，他特别喜欢一个角色 Lester，Lester 通过跟踪手机通话而找出了巴尔的摩的毒贩网。Stasio 想在伊拉克做同样的事情。

***

而 Stasio 不知道的是（他当时也不可能知道，因为他的安全许可是有限的）他的情报战想法已经被美国政府的最高层采用了。在国家安全高级官员与美国总统乔治·W·布什的 2007 年春季会议上，总司令授权国家安全局开始侵入伊拉克武装分子的手机和计算机网络。

伊拉克移动电话网络是一个潜在的情报金矿。萨达姆下台之后，手机合同是伊拉克第一批生意之一。因为无线通信比有线通信便宜，所以手机逐渐普及。根据与运作外国电信网络的美国电信运营商的协议，NSA 可以访问外国电信网络。这些电信运营商允许 NSA 访问其网络和其中存储的数据，并由此获得了丰厚的回报，一位前公司高管称，每个公司每年都获得数千万美元的报酬。

Stasio 只是庞大的黑客攻击计划的一员，是新型网络战争的先锋。之后，布什总统下达了命令，由战士和间谍组成的混合军队和情报部队对伊拉克进行日常攻击。其运作中心是巴格达北部的巴拉德空军基地的一个机库，这里曾经安置过伊拉克的战斗机。而此时，这里的大多数飞机是无人机。飞行员与 NSA 黑客、FBI 网络取证调查员以及特种作战部队（军方的精英突击队）一起工作。他们分成各个小组，进行无缝的精密合作。黑客从敌人的电子设备中窃取信息，并将其发送给分析人员，而分析人员则为部队制定出目标列表。当他们发动攻击时，无人机飞行员在空中监控，给地面部队发出相应的警报，这要归功于美国中央情报局开发的先进的摄像头和其他传感器。有时，无人机飞行员也会进行导弹射击。

在持续了 4 年的伊拉克战争中，美国第一次找到了真正有效的战略。

当攻击结束后，部队从占领的地方或抓获的作战人员身上收集更多情报，包括手机、笔

记本电脑、U 盘、通讯录、被称为“口袋垃圾”的纸片（这些纸片可能只写有一个名字、一个电话号码，或者一个物理或电子邮件地址）。部队将收集的信息反馈给基地的分析人员，分析人员将信息整合至数据库并使用数据挖掘软件寻找与其他作战人员(无论是被关押还是在逃）的联系。他们密切关注作战人员如何获得报酬，包括伊拉克之外的渠道--伊拉克、叙利亚、伊朗和沙特阿拉伯。

部队每天都能够抓获 10 到 20 名作战人员。整个恐怖分子网络就这样逐渐被了解，美军已经能够像敌方那样思考和行动了。恐怖分子不采用垂直结构，而是采用网络形式，每个成员分别应对地面上的情况，他们创造了一种新的战争形式。

NSA 已经建成了基础设施来入侵通信网络。911 恐怖袭击之后，NSA 建立了新的监听站和收集点，以监控恐怖分子的网络空间，包括通话、电子邮件和其它数字通信。许多新的访问点是美国主要电信运营商的办公室和交换站。追踪特定叛乱分子手机的分析人员可以看到手机登录网络的时间。该分析人员将该信息传达给地面部队，然后地面部队截获无线信号（如果地面部队距离太远，则会利用飞机和卫星来捕获信号）。所有这些数据被很快整理，并由此定位目标，可以具体到街道、建筑，甚至是他打电话或发短信的公寓。

***

该新型情报战略还有另一个支柱。除了收集伊拉克的所有电子通信，并用它来找出作战人员和资助者的位置，NSA 开始自己操控通信途径—叛乱分子的手机和电脑。

美国黑客给叛乱分子和轰炸人员发送虚假短信。这些消息会告诉收件人“在这个街角碰面并计划下一次攻击”或“到道路的这个点安置设备”。当作战人员到了那里，等待他的是美军或从数千英尺高空的无人机上发射的地狱火飞弹。

NSA 的黑客和分析人员与伊拉克的地面部队合作，渗透基地组织的网站和服务器的网络，美国人将该网络称为方尖碑（Obelisk）。方尖碑其实是基地组织的内部网，恐怖分子在该网络上发布宣传视频，以及发动圣战的行军命令和计划。他们甚至发布行政材料，包括支出账目和个人备忘录。方尖碑是叛乱分子的 C&C 系统。一旦进入方尖碑，NSA 黑客会在圣战论坛中植入恶意软件，诱导读者点击将在其计算机上安装间谍软件的链接。间谍通过方尖碑获知基地组织的秘密，以及渗透到其部队的方法。

Stasio 致力于自己的情报任务，并取得了令人印象深刻的胜利。他和他的团队使用信号情报来定位叛乱分子的巢穴，将其清除，并最终得以追踪相关人员的整个网络。他们发现了

负责制造用于恐怖分子自杀式袭击的背心，并追踪到他的工作室。当部队一脚踢开房门后，发现一名女子已经穿上了这种致命的服装，炸弹制造者和人肉轰炸机都被逮捕。

该小组发现了数千枚爆炸成型弹丸（EFP），这是他们在伊拉克发现的最大的库存。EFP 可以在一段距离之外发射，并且能够穿透装甲车（战士为免受传统路边炸弹的伤害而驾驶的车辆）。这些 EFP 被藏匿于一所不起眼的房子的一个房间里。 Stasio 和分析人员发现一个外国人在训练伊拉克人制造这种致命的炮弹，这个外国人也被抓获了。

Stasio 只是一个年轻的军官。但在他担任分析员的新角色后，他必须了解炸弹的位置，谁制造了炸弹、谁资助了炸弹的制造。每次他的上级与酋长或地方领导人会面时，Stasio 需要向其介绍政治背景，环环相扣的有时甚至可以互换的联盟的复杂性，美国希望利用这些信息赢得更多伊拉克人的“支持”。

据他所知，在战争中从来没有任何这样低级别的军官被允许获知如此多的战术和战略信息，他不仅可以了解战场情况，也能够了解战争的地缘政治现实。通常，这种分析是由更高级别的军官执行的。

他的同僚取笑他：“Bob，你今天向总统做简报了没？”

他把这当作一种恭维。

***

随着作战步伐的加快和效果的显现，NSA 投入了堪称最训练有素的网络战士。他们任职于一个称为“获取特定情报行动办公室”（TAO）的机构。顾名思义，他们设计定制的工具和技术来攻破计算机。TAO 拥有美国最隐蔽和最顶尖的黑客（只有几百名），其中许多人经历了多年的 NSA 培训，有的培训是在 NSA 帮助编写课程的高校中进行的。

在一个成功的行动中，TAO 黑客把目光投向了“伊拉克伊斯兰国”，这是一个成立于 2004 年的叛乱组织，宣誓效忠并拥护基地组织。该组织与美军作战，但是它也恐吓和杀害平民。仅在 2007 年，该基地组织分支就杀害了 2000 名伊拉克人，并占领了巴格达南部的多拉区，试图在那里实行伊斯兰法并成立新的“酋长国”来控制人们。曾住在多拉几十年的当地基督徒宁愿逃离家园，也不愿生活在如此苛刻的宗教统治之下。新的酋长国的一员敲开了一个基督教的家门，告诉他，如果他想留下来，他可以缴纳赋税或皈依伊斯兰教。否则，他必须放弃他的房子；基地组织成员表示帮助其搬运家具。

TAO 黑客瞄准了该基地组织的领导人。在巴格达作战中，TAO 黑客挖掘出了恐怖分子个人帐户中的草稿形式的电子邮件，恐怖分子这样做是为了让同伴获得电子邮件而无需通过互联网发送。这是恐怖分子用来规避检测的常用伎俩。TAO 已经破解好几年了。

对于 TAO 来说，攻破高级基地组织领导人的通信网络有助于打破恐怖组织对巴格达周围居民区的控制。通过一个帐户，TAO 帮助美军捕获或击毙了至少 10 个这样的高级领导人。当一个被称为“箭头撕裂者行动”的大型行动在 8 月中旬结束时，该地区的大多数叛乱活动已经停止了。到了 11 月，基地组织已经离开了多拉区域。

该情报机器不断地赢得胜利。据报道，2008 年上半年，基地组织在伊拉克发动了 28 次爆炸和其他攻击，而上年同期的数量则是 300 次。恐怖组织造成的平民伤亡人数也直线下降，从 2007 年的 1500 人到 2008 年上半年的 125 人。前军事情报官员将对基地组织高层的网络攻击比喻为“斩下了蛇头”。

“我们采取行动以进入他们的通信系统和 C&C 系统，恐怖分子和叛乱分子正是通过这些系统来计划对美军的攻击”，他说，“这是任何成功行动的关键”。

在持续了 4 年的伊拉克战争中，美国第一次找到了真正有效的战略。战争的全面成功最终使得美军得以离开伊拉克，参与战争的历史学家、指挥官和战士将成功归于三个主要因素。首先，地面增派部队帮助保护了最暴力的地区，击毙或捕获了叛乱分子，并保护了伊拉克平民。城市变得不再那么暴力，人们感到更安全，更倾向于帮助美国。第二，被基地组织的残暴战术和宗教法律激怒的反叛组织转而反对恐怖分子，或者收到美军的好处而支持美军。这种所谓的逊尼派觉醒包括 80,000 名作战人员，其领导人公开谴责基地组织，并赞扬美军试图改善伊拉克人民的生活水平。

全面胜利的第三个因素，也可以说是最关键的因素，是 NSA 和战士们进行的一系列情报行动。前情报分析员、军官和布什政府高级官员表示，网络作战打开了新型情报获取方法的大门，并将获得的情报用于地面作战。美国间谍从敌方计算机和手机中获取了敌方动向和计划信息，为美军提供了寻找敌方作战人员的路线图，有时甚至能够直接找上门。这是有史以来发明的最复杂的全球跟踪系统，而且效率非常之高。

Gen. David Petraeus 是伊拉克所有联军的指挥官，他将持续到 2008 年夏的新型网络战称为“美军取得显著进展的首要原因，直接消灭了战场上的近 4000 名叛乱分子”。伊拉克战争的浪潮终于朝着对美国有利的方向了。情报行动后来被应用于阿富汗战争，“通过识别和消

除战场中的极端主义威胁，拯救了美军和盟军的生命。”后来，NSA 将其在战争中开发的技术整合到其他情报行动中，用于追踪世界各地的恐怖分子、间谍和黑客。NSA 与军方在伊拉克战争中结成的同盟将永远地改变美国的战争方式。