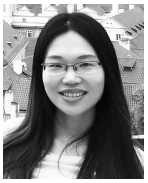
DOI:10.15997/j.cnki.qnjz.2020.28.028

● 王　茜／编译



跟踪和阻止错误信息传播的科学前沿

数据科学家研究错误信息的传播

英国数据科学家萨拉·杰恩·特普使用网络安全工具来跟踪虚假信息。她的目标是阻止它破坏人们的信念，并制止那些危险的谎言的传播。

2018 年 6 月上旬，她接到一项任务飞往佛罗里达州坦帕市，参加美国军方举办的军事演习。在纪念诺曼底登陆周年之际，美国特种作战司令部聚集了一大批专家和士兵进行头脑风暴实验：如果今天要发生诺曼底入侵，那会是什么样的结果？ 1944 年的行动之所以成功，很大程度上是因为盟国花了将近一年的时间来植入虚假信息，通过伪造无线电广播，说服德国人在他们不曾去过的地方集结部队，甚至在关键地点部署了伪装坦克。当下的世界，使用当今的社交媒体工具，将如何欺骗敌人？特普在佛罗里达度过了这一天。科学家集思广益如何愚弄现代军事战役中的敌人，尽管她从未知道结果会如何。她与邀请她的海军司令帕布鲁和网络安全专家马克·罗杰斯探讨了现代信息欺骗如何带来新的危险，例如，利用普通人通过社交媒体进行虚假和错误信息传播的运动。

科学家讨论如何创建自己的程序脚本来跟踪和阻止错误信息。如果有人发起一项社会运动，他们想知道信息是如何传播的。如果全世界的人都开始引用相同的奇怪理论，那么他们想要了解背后的原因。对于黑客，数据科学家习惯于通过分解文件包了解其工作原理，例如在恶意软件中使用潜伏在代码中的文件，并追溯到俄罗斯的犯罪集团，或者对拒绝服务攻击进行反向工程以找到防御的办法。他们意识到，作为网络安全问题，错误信息可以用相同的方式处理。

人的信念可以被黑客入侵

科学家们坚信必须找到一种分析错误信息运行模式的方法，以便研究人员能够了解其运行方式，并能够加以应对。不久之后，特普帮助国际安全专家、学者、新闻工作者和政府研究人员组成了一个国际小组，共同致力于这一项目。在特普看来，恶意软件和影响力活动之间存在一个关键区别。病毒通过易受攻击的端点和计算机网络的节点传播。但是使用和传播错误信息时，这些节点不是机器，而是人。“人们的信念可以被黑客入侵。”特普说，如果你想防范攻击，则必须找出网络中的薄弱点。在这种情况下，该网络就是全体网络使用者。

特普的职业生涯开始于英国政府的国防研究工作。她的第一项工作是开发可将声纳读数与海洋学数据和人类情报相结合的算法，以帮助定位潜艇。她说：“在大数据流行之前，就已经存在大数据。”她对数据如何塑造人的信念，以及如何应用于操纵人的信念产生了浓厚兴趣。当时是在冷战时期，要保持优势就意味着需要知道敌人将如何欺骗自己。冷战结束后，特普将工作重心转移到了灾难应对上。她成为危机地图绘制者，通过对地面来源信息收集并综合数据，从而对真实情况进行描述。正是在 2010 年海地地震和 BP 石油泄漏等灾难期间，当特普在工作中收集来自媒体实时数据时，她开始注意到，那些似乎故意发布的虚假信息的目的就是在已经混乱的时局中创造更多混乱。有一篇文章援引俄罗斯科学家的话说，英国石油泄漏将使海床坍塌并引起海啸。最初，特普认为它们如同阻塞数据流的垃圾一般是孤立的事件，然而，随着 2016 年大选临近，她和其他研究者开始清楚意识到，虚假信息活动是由那些老练的竞争对手发起的。

追踪和防御错误信息

在坦帕，特普和布劳尔迅速着手策划对错误信息的防御。他们着眼于小的线索，例如病毒帖中的特定字体或拼写错误，或者那些在网络中的最活跃的 Twitter 账户的特征等，去揭示这些别有用心的活动的起源、范围和目的。正如特普所说，这些“人为产物”是数据袭击后残留下的细小印记。他们认为，对于信息安全界的人来说，最有效的方法是找到一种追踪残留下的那些细小印记的方法。

由于网络犯罪分子倾向于从通用的技术清单中收集信息并加以利用，因此许多网络安全研究人员使用一个被称为 ATT & CK 框架的在线数据库来分析黑客入侵，这就好比是一个黑客在不断传播各种形式的混乱活动的目录。特普和布劳尔想要建立相同类型的数据库，但这一数据库是为了提供错误和虚假信息。为了充实他们的数据库，他们成立了错误信息安全团队，分析了先前的竞选活动，从 2015 年的 Jade Helm 15 军事训练演习（在社交媒体上被扭曲为试图在得克萨斯州实施戒严）到俄罗斯关联的 Blacktivist 账户，该账户在 2016 年大选中试图解析每类竞选活动的运营方式，对传播内容进行分类，并确定其中反复出现的策略。例如，来自网络影响力者的推送是否传递了信息合法性和影响力？是否从另一个竞选活动中借来的标签可以影响那些追随者？

科学家认为，一旦他们能够识别出某种模式，还将观察到信息的阻塞点。

在网络战争中，有一个从军方借用而来的概念被称为“杀伤链”，在确定攻击的阶段，可以预见它们将要做什么。如果能以某种方式中断该链，则攻击将失败。错误信息安全团队最终基于 ATT & CK 框架开发了一种用于对错误信息技术进行分类的结构，并将其称为 AMITT（错误信息及影响力对抗策略与技巧）。到目前为止，他们已经确定了 60 多种错误信息技术，并将它们映射到网络攻击的各个阶段。技术 49 已经被广泛使用，其中包括使用网络机器人或水军大量发布信息，并通过将其他信息淹没来终止对话。技术 18 是一种有针对性的付费广告。技术 54 是 Twitter 机器人的增强款，但这一数据库才刚刚起步。

去年 10 月，这一研究团队将 AMITT 集成到了一个国际性的开源威胁信息共享平台。这意味着任何地方的任何人，只需单击几下，即可指定某种正在发挥作用的战术、技术和程序，就可以加入错误和虚假信息的宣传活动中。特普和布劳尔使用“认知安全”一词来描述这一防止恶意因素入侵人们信念的工作。他们希望世界网络安全团队和网络威胁研究人员能够承担起这项工作，无论是为了管理品牌声誉，防止市场操纵还是保护平台免受法律风险，他们预见到这种需求未来将会不断增长。

错误信息传播的目标人群

很多美国谈话类广播节目会讲述一个国家陷入危机的长篇小说，这是一个毁灭美国的自由主义阴谋，并意图破坏人们原本的生活方式。在网上，左派人士也不断受到生存威胁的困扰。特普认为，这种恐惧和分裂使他们成为错误信息的理想目标人群。具有讽刺意味的是，能破解这些恐惧和信念的人通常本身是典型的敌对方和局外人。无论是为了破坏政治体系稳定还是仅仅为了赚钱，错误和虚假信息的传播一般都存在具体目标。然而，信息接收者通常看不到全局。

今年 2 月，西雅图的一名医生告诉特普，有一种不寻常的肺炎正在该地区蔓延。几周后，西雅图成为美国第一个冠状病毒传播的地区，不久之后，疫情大流行就开始与人们所说的“信息流行病”同时发生，带来了一阵虚假信息随疾病蔓延的浪潮。其中，有一则被广为流传的 Facebook 视频声称该新型病毒是美国制造的生物武器，该视频提供了一个使用 AMITT 数据库的机会，因此布劳尔开始对视频的特征文件进行分类，视频中使用了卡斯蒂利亚西班牙语。其中摄像机摇摄镜头展示了叙述者声称针对病毒突变的某些专利号，布劳尔查阅了专利并不存在。当他跟踪视频的路径时，发现该视频已被 Facebook 上的袜子木偶账户共享。他打电话给南美和拉丁美洲的朋友，询问他们是否看过该视频，发现该视频已经出现在墨西哥和危地马拉两个星期，然后才出现在阿根廷。当布劳尔观看视频时，他从 AMITT 数据库中识别出几种错误信息的技术。“创建伪造的社交媒体资料”属于技术 7。该视频使用了伪造的专家，看起来更加合法（技术 9）。他认为这可能是在为其他错误信息宣传打下基础（技术 44：播种失真）。

追溯错误信息的来源

与追寻恶意软件一样，追溯错误信息的来源也并非是一门精确的科学。卡斯蒂利亚西班牙语作为纯正的西班牙语，似乎旨在使视频在拉丁美洲的传播具有权威性。视频高产量代表背后的巨额财政支持。该视频首次出现在墨西哥和危地马拉，以及其发行时间（2 月是在迁徙的南美民工离开本国去美国进行春季播种之前），暗示该视频的真实目标可能是为了破坏美国的粮食安全。布劳尔认为，他们以其他人为目标来瞄准美国，这些是真正了解地缘政治带来后果的人。布劳尔希望在未来，研究人员可以看到类似视频如何在上一级进行传播，能够识别模式，并尽快进行破解。

今年 8 月，特普在家里看到一则视频，声称新冠病毒是世界卫生组织带来的恶作剧。令人惊讶的是，这一视频已经获得了将近 15 万的观看次数。她还看到一些瑞士网站宣扬知名美国免疫学家安东尼 · 福西质疑病毒疫苗会成功，以及宣传医生认为戴口罩是没用的。她的团队正在搜索是否存在链接到同一主机域的其他网络链接，确定网站上使用的广告标签，并追踪资金来源。他们对特定的短语和叙述进行分类（例如有人声称德国当局希望将感染了新冠病毒的孩子转移到拘留所中），寻找这些类似的叙述还在哪里出现过，并将所有这些内容输入数据库中，增加了数据库应对错误信息的能力。她对项目的发展势头持乐观态度，因为使用的次数越多，AMITT 数据系统的效率就越高。目前，该团队正在与北约、欧盟和美国国土安全部合作测试该系统。

特普对受到攻击的网络的力量保持谨慎乐观的态度。当人们要争取一些具体的事物时，他们就不太容易陷入与虚拟敌人的幻象战中。特普希望人们能够学会主动拒绝错误信息。在针对美国黑人乔治 · 弗洛伊德事件的抗议期间，特普的团队追踪了另一则谣言。其中有一个模因不断以各种形式浮出水面，是关于“小镇上的反法武装”在抗议中被驱逐的一个假消息。然而，一些保守的社区中有人揭穿了这个阴谋，这些人从某种程度上理解到其社区遭到了黑客入侵，他们需要捍卫自己的安全。因此，阻止那些危险的谎言来侵犯人们的信仰，最终的力量还在人们自己手里。

（本文原文为《One Data Scientist’s Quest to Quash Misinformation》，编译自 https://www.wired.com/story/data-scientist-cybesecurity-tools-quash-misinformation/。作者 Sonner Kehrt 为《连线》杂志自由撰稿人。编译者王茜为上海交通大学媒体与传播学院副教授，新媒体全英文国际项目主任，健康传播研究中心主任）