连网设备带来新的监控方式

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Connected Devices Give Spies a Powerful New Way to Surveil		
原文作者	Shay Hershkovitz, Roey Tzezana	**原文发布日期**	2017 年 1 月 19 日
作者简介	Shay Hershkovitz 是一名情报专家和战略家。https://il.linkedin.com/in/dr-shay-hershkovitz-6b96802		
原文发布单位	https://www.wired.com/2017/01/connected-devices-give-spies-powerful-new-way-surveil/		
原文出处	Wired		
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。		

连网设备带来新的监控方式

Shay Hershkovitz，Roey Tzezana

2017 年 1 月 19 日

对任何情报机构来说，网络都是最棒的礼物，这一点毋庸置疑。安全机构和商业实体可以轻松收集用户信息。每个互联网用户都处在监控之中。

幸运的是，在现实世界中我们仍然可以随心所欲，不必忍受无休止的监视。是这样吗？想必好景不长了。

随着物联网（IoT）的出现，在网络世界中发生的数据收集革命即将在物理世界中重演。物联网的设计理念是，日常物品可以无线收集和传输数据。无数物品能够连接到互联网：从路面上的瓷砖和墙上的混凝土，到我们的鞋子和衣服，甚至牙刷。这些物品都可以连网，而且很快就会将其信息上传到云端。

利用物联网实施监控正在获得美国情报界的认可。去年，前美国情报总监詹姆斯·克莱普（James Clapper）在接受《卫报》采访时表示，情报机构可能会利用物联网设备实施“识别、监视、监控、定位和追踪，并利用相关信息进行招聘、访问网络或获取用户凭证。”

这种方法说明美国情报界很关心这项新技术 新的数据收集和分析能力必将改变目前的情报范式，并创造一个新的范式。

新的情报范式诞生

美国国家情报局定义了六种基本的情报收集范式：信号情报（SIGINT），图像情报（IMINT），测量与特征信号情报（MASINT），人工情报（HUMINT），开源情报（OSINT）和地理空间情报（GEOINT）。

物联网将会带来第七种情报收集范式：时间情报（TEMPINT）。TEMPINT 不是一种狭隘的情报收集方法，不会侧重于某些情报源；反之，它是一种整体性的数据收集和分析方法。TEMPINT 假定大多数人和基础设施都会被监控，可以收集，存储和分析这些数据。

我们举例说明 TEMPINT 的作用：一名武装恐怖分子在拥挤的商场中攻击顾客。他在几分钟内就被击毙了，因此警方无法审问其同伙是谁，但他留下了一些痕迹。情报机构可以查看商场的监控录像，确定他是从哪里进入的，还可以查看停车场的监控录像来确定他的车。通常情况下，调查到这里就终止了。但是在物联网更加普遍的将来，分析人员可以利用遍布道路的摄像头和传感器收集的记录和信息，迅速地逆时间方向追踪恐怖分子的车辆。在完全连网的世界里，分析人员可以让时间倒流，确定恐怖分子见过的所有人，然后再对这些人进行“逆时间方向”分析。

一些数据在收集和存储时并没有什么目的性，而该方法正是利用了这些数据。在过去，数据获取颇为困难，数据存储的成本也很高，因此情报机构在数据收集方面非常挑剔。但是现在，连网传感器几乎无处不在，每个传感器都能不停地传输数据，而情报机构只需存储这些数据就行了。因此，情报机构获得了一个强大的工具：当发生新事件时，分析人员可以查看存储的数据，“逆时间方向”分析这些事件的发生过程。TEMPINT 平台类似于对整个世界进行录像，分析人员可以放大、暂停和回看这些录像，利用可穿戴设备收集的信息对每个人的健康状况和心态进行注释。

TEMPINT 面临着两个主要的技术挑战，目前正在解决。

第一个挑战是数据存储。执行 TEMPINT 意味着我们必须存储大量的数据以供将来查看。在 2019 年，物联网预计将产生超过 500 ZB 的数据（译者注：1ZB = 1 万亿 GB）。不过，情报机构可以只收集基础数据，包括：录音，位置和活动，监控摄像头的定期拍摄。此外，过去的几十年中，数据存储能力得到了大幅提升，这种趋势还会继续下去。

第二个技术挑战是从大量数据中过滤出所需的信息。这个挑战可以通过人工智能的快速

发展予以解决，神经网络可以识别图片和视频中的面孔、物品，甚至抽象概念。

是否应该获得 TEMPINT 能力？

有人可能会问：安全机构和商业公司是否应该获得 TEMPINT 能力？这个问题有些模糊，因为他们已经具备了初期的 TEMPINT 能力。毕竟，NSA 收集了大量在线传输和通过设备的信息。随着物联网的发展，各国政府将会利用它来监控公民，就像他们现在在网上做的一样。

可以理解，公民非常担心政府日益增长的监控能力。情报机构不应忽视这些恐惧；他们应努力减轻公民的恐惧心理。例如，当局可以利用人工智能引擎来识别潜在的恐怖分子，无需让分析人员审查数百万公民的详细信息。情报机构甚至可以公开一些算法，供公众监督。这种透明度有助于防止信息滥用，还可以增加一个由公众和看门狗组织实施的漏洞检测层。

不幸的是，奥巴马政府最近实施的变革允许 NSA 与其他 16 个美国情报机构共享收集的信息，而且不需事先实施任何类型的隐私保护措施。所以，现在的问题已经不是 TEMPINT 将来是否会被使用：它已经存在了，只是还比较有限。当局的监视意愿很强烈，虽然目前的技术仍然薄弱，但是其力量正在增长。我们应该把它看作是一种新的情报范式，并思考它的使用（这是不可避免的）将会对整个社会带来什么样的变化。在单一黑客恐怖分子能够造成巨大损害的时代中，我们必须随时随地进行监控。

情报机构经常被指责没有为未来的挑战做好准备。现在，他们可以利用物联网和 TEMPINT 范式提前做好准备了。迄今为止，这是情报机构应对敌人最重要的优势，也是民主国家的公民必须作出的妥协。