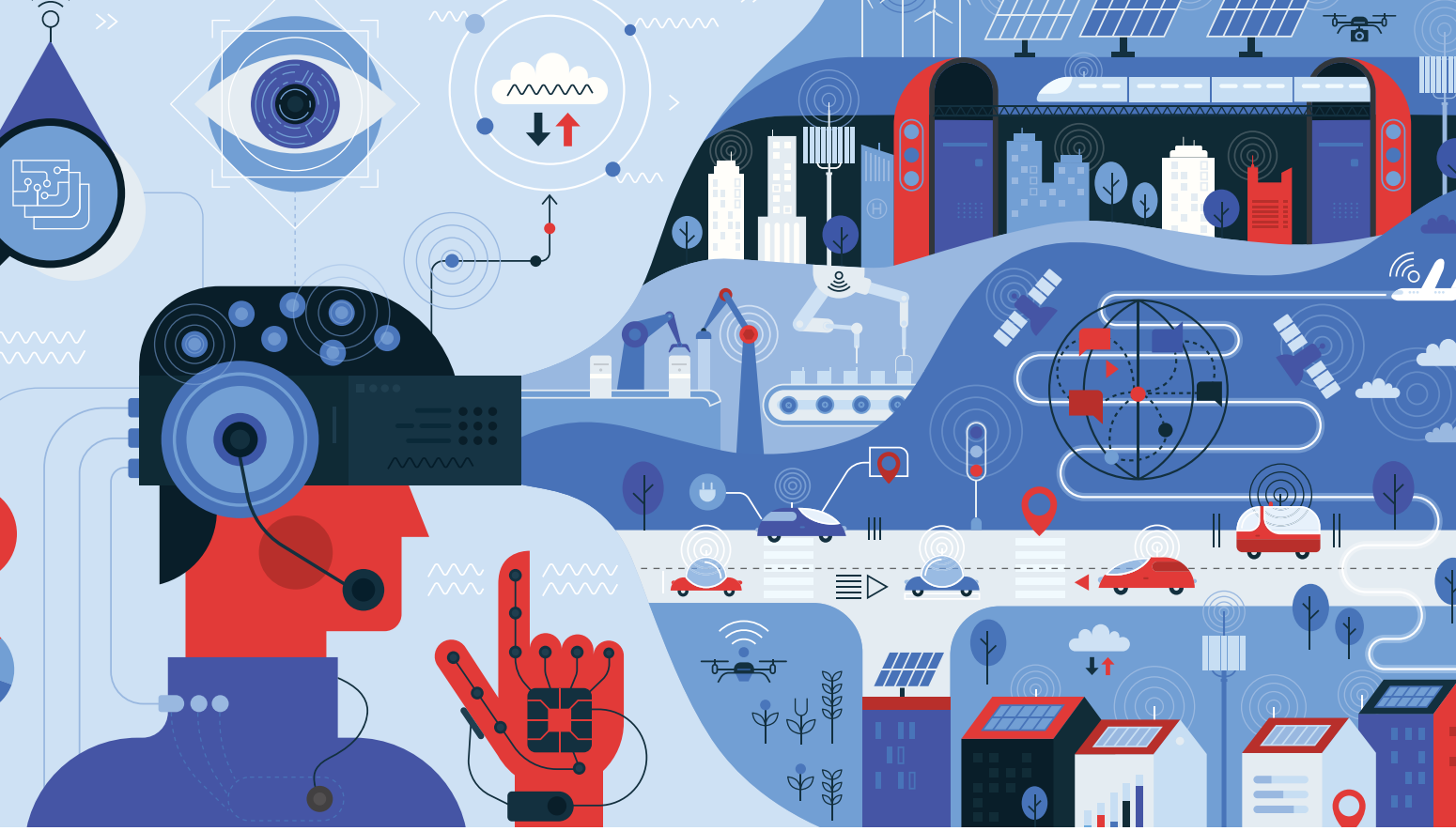

技术变革

全球向超级连接的时代转变，这在为全人类带来巨大机遇的同时，也产生了风险和挑战

赫尔夫·托普

新冠疫情封锁与科技改变了我们生活的方方面面，对于这些改变本身以及其将持续多久，每个人都有自己的看法。科技公司押注了长期趋势。它们正在做出迅速调整，以适应后疫情时代的世界——在这个世界，包括购物、学习、工作和社交活动在内的很多事情是在家中完成的，这其中很多都要借助所谓的非接触式技术，尽可能避免与现实世界互动。

近期，2021 年的消费电子展——全球最具影响力的科技活动之一——让我们窥见了未来世界的一端。现在的笔记本电脑完全是按照视频会议的需求设计开发的，它配备了多个摄像头、专用灯光和软件优化音频装置。此外，内置有蓝牙耳机和麦克风的 N95 口罩，搭载有微型显示屏的智能眼镜，这些设计让人们在保证安全的前提下开展社交活动。非接触式的门铃可帮我们在家门口控制细菌的传播——当有访客到来的时候会通知房主，甚至还可以检测访客的体温！

然而，技术进步并非富裕国家的专利，也并不局限于高科技产品。例如，在缺乏甚至完全没有医疗体系的低收入国家，大型科技公司正在研发开源的人工智能代码并用于医学影像分析工作——包括癌症的早期筛查，此举有可能会改变医疗行业的整体格局。远程医疗和远程教育的需

求日益增加，重新引起了人们对增强现实技术的兴趣。据联合国儿童基金会和其他组织预计，该项技术有望搭建一座桥梁，带领发展中国家文化水平不高的人群进入数字世界。技术的快速变革，使得世界变得更加智能、更加公平，伴随着技术变革，我们还应当将目光投射在基础设施、数字身份、新的数字风险等基础要素上。

超级卫星星座

以互联网卫星为例。新一代的超级卫星星座能够为全世界 53% 的发展中国家接入互联网，这能改变游戏规则吗？理论上讲，可以，美国太空探索技术公司（SpaceX）原计划发射 1.2 万颗近地轨道星链卫星，目前，已发射了 1000 多颗。这些都是近地运行卫星，可以将互联网信号发送至全球任何一个偏远地区，无论您是地处加纳的一个偏远村庄，还是身处荒芜的北极基地，它的信号传输品质以及传输速度都无与伦比。其他公司，例如一网公司（OneWeb）计划在今年一年内发射 650 颗卫星，与此同时，亚马逊（Amazon）的凯伯项目预计很快就会发射数千颗高速卫星。这项技术可以帮助全球多个国家，在互联网基础设施投资领域，跨越几十年实现联网目地。

根据国际货币基金组织的研究，撒哈拉以南的非洲地区的互联网普及率每增加 10%，实际人均 GDP 增长率就会提高 1 至 4 个百分点。鉴于这些地区有四分之三的人口目前还没有接入互联网，其 GDP 增长潜力巨大。任何一个国家若缺乏宽带连接，都将放大社会上的不平等现象。

目前，要建立地面互联网连接，不仅需要工期长达多年的大量跨境网络基础建设投资，还需要国家的“骨干”级互联网公司和“最后一英里”连接。据预计，仅在非洲，未来 10 年就需要花费约 1000 亿美元。近地轨道卫星公司承诺，将在未来两年内实现这一目标，而且成本仅是前者的很小一部分。每户家庭只需要安装一个小型天线和一个盒子就能上网。这些卫星甚至可以作为移动网络的“骨干”，考虑到人们更加倾向于手机上网，这会进一步加快高速网络的普及。

那么，这存在哪些难点呢？首先，全球卫星数量可能从目前的 3000 多颗增加到 20000 颗以上，对地面天文学产生影响。据预计，个人的最初成本大约是每月 100 美元——硬件需要另加 500 美元，对于贫穷国家的人来说这个价格过于昂贵，需要国家补贴。最后，如果实现宽带连接的时间比预期更快，政策制定者就必须了解它的影响，以及这个技术为公民所创造的价值。

例如，在以前网络资源不发达的地区，群众可能不懂互联网上使用的主要语言。如果政府不能提供基础的数字和金融技能培训，网络连接可能只能部分惠及这一群体。最重要的是，随着网络连接覆盖范围的拓展，诈骗与数据滥用等数字威胁问题也越来越多。在接下来的两年里，新一代的高速网络卫星有可能会改变数十亿人的生活。国际组织、开发银行和各国政府要抓住这个新的机遇。但同时，也必须加强监管，落实数字技能培训，还有及时地转变人们的思维方式。

数字身份

接下来是数字身份技术。在新冠疫情促使全球加速向更加互联的时代转变之前，人们便已将数字身份技术看作最重要的技术趋势之一了，这对发展中国家而言尤其如此。根据世界银行的数据显示，全世界有 11 亿人缺乏个人备案或提供验证身份的凭据。多年来，许多国家都曾尝试过复制印度的阿达哈尔数字身份证以及爱沙尼亚的国家身份证电子识别系统的成功模式。其好处包括提高政府在预算和选举方面的透明度，打通政府援助渠道，扩大基础金融服务的覆盖范围，特别是对于那些无家可归或没有个人备案的人而言。多年来，由于国家协调不力、数字素养有限等诸多挑战，使得网络普及十分缓慢。网络安全问题、数据隐私问题、对政府提供的技术的不信任等，也推迟了数字身份证在许多国家的部署工作。正是这些尚未解决的挑战使数字身份证计划被搁置一旁。

但新冠疫情迫使各国政府或是迅速克服困难，或是绕开这些问题，向最弱势的民众提供了他们急需的财政援助和其他形式的帮助。现在时机已经成熟，各项部署国家数字身份证的有利因

设计：ISTOCK/ DRAFTER123

对于寻求拥抱数字转型的国家来说，网络犯罪只是众多需要应对的数字风险之一。

素，包括建立可以体现社会经济指标的可靠数据库，已经超过了不利因素。

基础技术现在已经相当成熟。例如，安全性和加密算法——双重验证、非对称加密等安全加密算法——提高了数据的完整性和私密性。人工智能、机器学习和内置在移动设备中的生物识别传感器可以显著地减少诈骗活动。这些技术还可以通过扫描用户指纹、面部或声音来简化用户体验。此外，最近还出现了数字身份证开源软件、基于开放应用程序接口（API）的解决方案、国际标准等，这些都降低了国家数字身份证计划的实施成本。

技术供应商已经先行一步，新一代的数字身份证解决方案正在迅速涌现。基于区块链的身份验证技术的早期测试，在一些国家风头正劲——其中包括爱沙尼亚。这项具有潜在突破性的技术可以将数据的控制权和所有权从政府手中转移到普通公民手中，同时保留政府签发身份证件以及查验身份并提供相关服务的权力。

但滥用数字身份的风险和可能性仍然存在，需要政策制定者和监管机构持续关注。本次新冠疫情无疑凸显了数字身份的有利一面，但当与追踪应用程序等其他技术结合起来运用时，也为用户带来了隐私泄露风险。无论使用哪种技术，成功的数字身份识别系统必须满足安全、包容和互操作等功能要求，以便向数十亿没有身份证件的用户传递它的颠覆性影响。

管理数字风险

新冠疫情使数字技术在全球的普及实现了跨越式发展，有的人说数字技术的发展进程至少加快了五年。另一方面，如上所述，数字风险也同样在加速。由于越来越多的人使用个人电脑访问企业系统，企业现在面临的网络威胁也越来越多。接触者追踪应用程序加剧了数据隐私和公共卫生政策目标之间的紧张关系，给监管机构和政策制定者提出了难题。黑客利用人们对病毒的恐惧和焦虑心理，引诱人们参与网络钓鱼骗局，并诱使他们下载恶意软件。更加令人不安的是，在新冠疫情期间，黑客曾向医院发起了勒索软件攻击，并试图窃取疫苗公司的知识产权。

这并不是什么新鲜事：在新冠疫情暴发之前，人们的网络风险意识就在逐渐增强。地缘政治的紧张局势以及新出现的网络攻击力，不仅让国家和非国家势力受到鼓动，也模糊了间谍和恶意黑客之间的界限。世界经济论坛甚至在 2019 年就意识到了这一威胁，将网络安全列为一项全球风险，风险等级仅次于气候变化。

但网络威胁的范围和环境在迅速改变。对于寻求拥抱数字转型的国家来说，网络犯罪只是需要应对的众多数字风险之一。不仅仅是美国，每个人都应该清楚技术在放大虚假信息中的角色。专家们担心虚假信息——由人工智能制作的深度伪造性视频，其效果与真实拍摄的视频一样——可能会传播难以揭穿的谎言，加剧政治紧张局势。人们对人工智能的担忧，都是根植在现实问题当中的。这些问题包括，自动化替代某些工作岗位的速度比预期更快，人工智能放大了性别和种族偏见，以及人工智能存在所谓的黑盒问题——也就是人工智能得出了连开发者都无法解释的结论。

全球向高速连接的世界转变，是数十亿普通民众获得更好的教育、医疗、就业和金融服务的一个巨大契机。这十年我们将目睹不断加速的数字化进程、更加复杂的数字问题，以及不断变化的数字风险。问题是：政府能否灵活地提高执政能力，迅速地采取更加全面的风险监管办法和数字战略，在限制风险的同时收获这种数字化进程加速所带来的好处？ FD

赫尔夫·托普（HERVE TOURPE），国际货币基金组织首席数字咨询官。