

访谈

瓦伦汀·韦伯
何流

瓦伦汀·韦伯 (Valentin Weber) 博士现任德国外交关系协会 (DGAP) 地缘政治、地缘经济与技术中心高级研究员，同时也是伦敦政治经济学院 IDEAS 智库的中国前瞻研究员

何流是斯坦福大学胡佛研究所研究员，目前与胡佛档案馆合作开展海外中国问题专家个人口述史项目，创办并编辑 Peking Hotel 新闻和播客。他拥有牛津大学学士学位和清华大学全球事务硕士学位

中国民主季刊

第3卷 第3期

2025年7月

CC-BY-NC-ND

自由、免费转载分发，但须注明
作者与出处，并不得修改及商用

数据中心型专制主义与民主的数字未来



瓦伦汀·韦伯



何流

编按：中国共产党正在利用人工智能监控、神经技术、量子计算和数字货币等前沿技术打造数据中心型专制主义，对社会进行全方位控制。更令人担忧的是，这些新兴技术也正在被中共输出到世界各地，威胁全球的民主价值和人权保障。瓦伦汀·韦伯博士是研究这一重大议题的权威学者，长期追踪中国数字专制主义的发展与全球扩散。他提出的“数据中心型专制主义”(data-centric authoritarianism) 概念，精准地捕捉到了当代专制体制运作的新特征。受《中国民主季刊》的委托，斯坦福大学胡佛研究所研究员何流先生对韦伯博士进行了专访。本次访谈围绕韦伯博士最新发表的重要报告《数据中心型专制主义：中国前沿技术的发展如何使镇压全球化》(Data-Centric Authoritarianism: How China's Development of Frontier Technologies Could Globalize Repression) 展开¹。

“数据中心型专制主义”更多涉及线下世界

何流（以下简称何）：能否谈谈是什么让你开始研究中国的数字专制主义，

特别是数据中心型专制主义？是否有某个特定事件让你意识到这一威胁的紧迫性？

韦伯（以下简称**韦**）：我第一次接触这个话题是通过我当时在牛津的博士生导师乔斯·赖特（Joss Wright）博士。他当时正在研究中国的信息控制环境，着眼于中国审查制度的地区差异。

通过我们的对话，我们开始讨论俄罗斯和中国的信息控制方式。这就是我博士论文主题的由来——比较中国和俄罗斯的数字专制主义模式。随着时间推移，我深入参与了互联网自由社群，这让我大开眼界。我学到了很多关于人们如何研究这个话题的知识，从那以后，我一直在从事这方面的工作。

何：你创造了“数据中心型专制主义”（data-centric authoritarianism）这个概念。它与数字专制主义（digital authoritarianism）有何不同？这又与传统的监控国家有什么区别？

韦：数字专制主义主要是在网上进行的专制主义——社交媒体审查和监控，追踪支付宝上的支付行为等等，更多是关于在线的专制主义。而数据中心型专制主义会影响线下的人们。数据被用来对实地的人们产生实际影响，特别是在城市中。人们的行动因此受到限制。这就是我想强调的“数据中心性”。

此外，我们最近看到了大量数据的扩散。以前，许多数据是孤立的，存在

于各自的信息孤岛中。现在它们正在被整合。

何：所以你说的是，数字专制主义涉及互联网，而数据中心型专制主义既有数据收集的线下部分，也有监控的线上部分，还包括量子计算和神经技术等非互联网技术？

韦：所有技术。技术对物理世界的影响越来越大。在 2000 年代初期，主要是关于万维网，中共真正关注的是在线平台上的审查。但在过去 10 年左右，这种情况确实发生了变化。

何：从哪个意义上说呢？

韦：大量数据现在可以导致对人们的持续追踪。这不仅仅是关于他们的在线行为或在论坛上发帖 —— 而是使用手机追踪他们的位置，找到他们，命令他们不要离开某个区域。越来越多地涉及这个方面。

何：我有时从极权主义失败模式的角度来看待这些技术。极权主义意味着国家对社会的完全控制，但存在失败点：外部竞争（如美国对苏联）、来自异见人士的内部抵抗、可能导致政权颠覆的精英分裂，以及每个极权国家都难以解决的接班人危机。

从你的研究来看，数据中心型专制主义如何与极权主义的这些失败模式相互作用？它是否强化了政权？同时是否开启了新的弱点？

韦：一方面，新兴技术在国际上强化了中国。他们正在提出技术治理的替

代模式，为自己的目的使用在线技术，向世界和其他独裁者展示他们不必采用民主制度就能实现经济增长。

在国内，他们使用“科学治理”(scientific governance) 这个短语，声称他们基于数据做出治理决策。这使得更难责怪特定的中共精英，因为他们是在“听从数据”。这可能使政权继承更容易，因为政策将保持不变——每个人都在听从于技术。

此外，它使专制主义更强大，因为历史上专制主义失败的原因是缺乏来自基层的正确信息。现在他们收集人们的日常情绪，人们可以通过城市工具投诉街道状况和其他问题。他们得到关于治理如何发挥作用的即时反馈。他们可以调整反应——如果他们看到小规模抗议，他们不会做出反应，但他们会更大的抗议做出回应。

这帮助他们专注于那些能让他们政权保持权力的要点。所以在许多方面，技术确实赋予了权力，并防止了威权政权以前的失败。

何：政权的运作极其秘密，例如，中央宣传部追踪来自中国各地的信息流。我们如何知道他们使用什么技术来提高工作效率呢？

韦：有很多方法。直到最近，政府采购文件是一个非常好的来源。你可以看到地区和城市警察部门购买或维护的确切系统。但现在这个来源已经有所枯竭。

另一个来源是泄露。中国的很多数据泄露，因为保护不善。

最重要的是，我依赖的来源是公司公告。公司讨论他们的产品，经常谈论他们为特定警察部门供货的成功案例。这是一个非常好的来源，大多数公司继续这样做。它帮助我们了解他们在做什么。几年后，你会看到同样的产品被销往国外。

这就是为什么要通过观察中国内部发生的事情，来预测全球正在发生的事情——因为他们在出口之前，是为国内市场销售和开发的产品。透明度比我们想象的要高。

何：那么我们谈论这些信息是否会有消极后果？譬如中国政府读到我们的文章后，决定停止这些做法？

韦：他们知道这正在发生。关于政府采购文件和公司营销材料——有这么多公司，他们无法控制所有公司。我认为没问题。

通常，他们认为人们不会研究中文网站。他们认为因为是中文，所以没有人会去查看。此外，这是一个庞大的系统。不可能控制所有信息。

何：在我看来，巨大的反乌托邦未来，是这些数据中心型数字技术帮助独裁者长久掌权——通过宣传、监控、干部评估和晋升、军事技术，继承实现专制锁定。这也就是所谓的稳定极权主义 (stable totalitarianism)。如果有足够符合习近平世界观的人工通用智能 (AGI, Artificial General Intelligence)²，当习近平去世时，谁来接替他？答案是：AGI。AGI 就在那里，任何想要废黜 AGI 的人都可以被驱逐出去。任何与 AGI 保持一致的人都会得到巨大奖励。

到那时，AGI 就像现在的电力对我们一样。考虑到它与永久存在的价值和共产党的价值一致，它可能永远存在。你如何评估这种风险？我们是否面临这些技术的真正风险？

韦：在我们考虑那种风险之前，专制领导人如习近平还面临着许多其他风险。他们经常误判形势。即使拥有所有数据，他们也会实施错误的政策。我们在新冠抗议期间看到了这一点——清零政策是一个错误的决定。没有人预料到会有如此严重的抗议反应。许多这样的误判每天都在发生，AI 还没有达到能够防止这种情况的地步。

在 AI 成为真正的解决方案之前，还有许多障碍需要克服。为此，AI 也需要变得物理化，这将真正通过机器人实现。一旦我们有了由 AGI 驱动的机器人，这将成为更严重的威胁。目前，AI 仍然很大程度上是无形的——它还没有那么多地体现在物理存在中。当我们有了这种具身智能——即有了感知能力、运动能力和与环境进行互动的能力——的未来，它将成为威胁。

四种前沿技术

何：让我们谈谈你研究的四种 AI 监控技术。中共政权显然非常擅长使用相机、算法和采购进行监控，这可以追溯到很久以前。我们是否有证据表明国家利用这些来平息抗议，有时甚至在抗议开始之前？

韦：我们还没有这些技术应用于尚未发生的事情的证据，但我们有证据表明他们每天都在使用它。我们知道预测性警务 (predictive policing) 工具正

在厄瓜多尔、委内瑞拉、乌干达使用。无论是在国外还是在中国国内部署智慧城市的地方，它一定有些作用，因为它们继续购买这项技术。它们似乎相信它减少了抗议的可能性。

我们不能说它阻止了没有发生的抗议。但在近年来你在中国看到的所有抗议中，预测性警务都被用来不让它们发生或镇压它们。

何：如果抗议无论如何都发生了，这不意味着预测性警务失败了吗？

韦：你可以让某些抗议独自存在。网上有很多对中共的异议，但当这些帖子没有广泛传播时，他们不在乎。同样，如果地面上的抗议没有广泛影响——如果是小规模抗议——他们不在乎。他们需要为严重案件保留警力。这就是预测性警务如何帮助他们做出决定：在线参与的阈值在哪里？有多少人可以看到某事才需要审查它？

何：委内瑞拉和厄瓜多尔的例子是什么？

韦：委内瑞拉和厄瓜多尔从中国进口了全市监控系统。在厄瓜多尔，官员访问了中国，之后进口了那些庞大的监控系统。在那里，它主要用于高效通信——如果某个地区发生事件，政府可以部署警车。这就是中国提供的监控和控制机制的类型。

何：我们如何踏过这个道德雷区？一方面，有人可能会说这是使警察更高效、使城市更安全的正常警察技术。另一方面，我们看到这个系统被滥用的明显潜力——压制异议、监视无辜公民、被政客用于自己的目的。我们

在哪里划线？

韦：这些技术已经被出售给民主政权，包括出售给许多欧洲国家。我们知道它们正在法国部署。智慧城市以前也被出售给一些德国城市。所以它们也被民主系统使用——这取决于它们如何被使用。

但仍然取决于你把技术给谁。如果你把它给专制或混合政权，那里没有权力制衡，那就不同了。我们看到华为帮助乌干达警察破解反对派政客的手机。这是另一个步骤——协助他们的专制努力。

何：在 2019 年香港抗议的案例中，我们既看到了一个监控国家的操作，也看到了与其对抗的积极努力。虽然民主运动最终失败了，我们是否可以从 2019 年香港学到关于社会与技术的有效对抗策略？

韦：当时，我们在香港学到了很多关于中国正在使用的技术——面部识别技术、间谍软件、移动设备跟踪器，等等。我们学到的主要事情是没有“简版中国”(China Lite)；在监控方面，香港是不会被区别对待的。这对台湾也非常有启发性，让他们知道在中共统治下会面临什么样的未来。

另一点是，世界各地的许多人都受到香港人斗争的鼓舞。它在今天仍在世界各地产生回响。看到人们抵抗是鼓舞人心的。

何：研究这些东西时如何保持良好的精神状态？这一切都相当令人沮丧，不是吗？

韦：当然，这是一个相当悲观的研究领域。其他人有不同的方法，对我来说，积极的一面是我能够揭露中国公司的做法。我正在研究监控基础设施。与人权组织每天遇到个案相比，我离现实的直接距离更远一点，不会立即了解受害者的感受，所以也少一些沮丧。

何：在你研究监控技术时，是否有“灵光一现”——某些事情让你觉得“就是这个”？

韦：是的。一个是“城市大脑”(city brains)。我第一次偶然发现这个术语——城市大脑是智慧城市的演变，主要是使智慧城市更智能的 AI 组件。我的“灵光一现”是几年前遇到那个术语。

今天，如果你看看这个术语，它无处不在——在中国媒体和警察部门中被提及。技术已经传播开来。看到我早期遇到的东西，当时人们认为它听起来像科幻小说，但现在已经成为一项主要技术。

何：你是如何得出报告中的四大技术框架的？我相信你考虑过这个特定框架的替代方案。你能谈谈那个过程吗？

韦：当然有很多新兴技术。对于这篇论文，我必须与编辑们，包括国家民主基金会 (National Endowment for Democracy) 的贝斯 (Beth Curley) 一起决定。我们决定了这四个，因为它们似乎对人权有最大的潜在影响：量子计算、神经技术、人工智能和数字货币。它们也反映了去年国家民主基金会有一个研讨会。基于那个研讨会，我写了报告。所以它既反映了这些技术的潜在影响，也反映了作为这份报告基础的研讨会。

我们也更强烈地关注了 AI 审查。AI 监控是我们关注的，但 AI 审查将是另一个。

何：在你列举的四个科技之外，机器人技术也是一个重大科技。

韦：机器人技术是一个，卫星技术可能是另一个——它如何影响自由，还有生物技术——关于 DNA 基因测序的一切。这些是其他的事情，但我们专注于那四个。

何：神经技术 (neurotechnology) 是个听起来像科幻，但实际上比人们想象的更接近现实的领域之一。这个领域的发展现状是什么？中国在神经技术方面有多先进，特别是在专制、反乌托邦用途方面？

韦：他们处于研究的前沿。在论文中，我区分了非侵入性和侵入性脑神经技术。目前最大的威胁来自非侵入性技术——你可以戴在大脑上测量脑电波的头戴设备。中国警方已经在研究这些，以了解如何在审讯环境中使用它们。在全球范围内，神经技术仍在兴起，但我们已经可以看到中国警察大学正在积极考虑和研究的警察用例。

何：侵入性呢？

韦：侵入性仍然更遥远，因为它仍然是一项非常新生的技术。当你将芯片插入大脑时，了解人们在想什么仍处于早期阶段。在 10 亿人的庞大规模上，很难想象他们能够在未来 5 到 10 年内通过直接访问大脑来实施监控。

脑电波监测技术的一个后果是识别情绪。目前，他们主要通过相机进行情绪识别，尽管这是否真的能显示人们的情绪是非常有争议的，这在科学上没有得到证明。

何：这与安全和监控国家有什么关系？

韦：就情绪识别而言，如果你在审讯某人时看到他们害怕，你可以推断他们有什么要隐藏的，或者如果他们对某些问题有某些情绪反应。在公共场所，如果你看到某人激动，你可以预防性地拘留他们，试图防止情况升级。

何：还有这样一条线，国家使用这项技术来阻止抗议，但他们也可以使用它来阻止恐怖分子——这就是他们会说的。

韦：这取决于如何定义恐怖分子和罪犯。许多人说技术是中立的——在很大程度上这是真的。但中国公司的技术具有识别维吾尔人和穆斯林少数民族的功能。那就不是中立的技术。如果你进口那项技术，它对它追踪的内容和识别的人有预定义的规范，我认为这种技术在所有情况下都不是中立的。

何：在中国，有关于神经权利 (neuro-rights) 和自由意志的讨论，也就是中国内部对如何使用这项技术存在不确定性。外部世界是否有办法干预或将对话引向更健康的立场？

韦：中国存在保护个人隐私的法律规定，但它们只适用于公司，不适用于国家。那些看起来良性的立法，但事实上它并不良性，因为国家拥有完全

的监控能力。我们将无法改变这一点。我们唯一能影响的立法是，中国如何监管私营部门或私营公司需要遵守什么。

何：我有这样的心理框架，即国家经常不知道它想要什么，也不计划某些技术的发生。但公司有明确的利润动机来发明各种工具和花哨的小工具。

鉴于这种动态——国家采购，但公司自主创新，试图猜测国家想要什么，发明各种花哨的技术，甚至可能发明国家没有意识到的需求——可以做什么来破坏国家和公司之间的这种微观动态？

韦：一方面，国家发布公司需要遵守的某些规范和法规。如果要建立重点人员的国家数据库，公司需要开发与之兼容的技术。但除此之外的一切真的是中国公司在创新。它们可能比国家官员或警察部门做出更明智的决定，因为真正了解技术的是公司——对它们来说，这不是黑箱。

我们如何影响它们？很难。美国试图将这些中国公司列入制裁名单，这可能会影响他们在国外的业务，但对中国国内的影响不大。对中国国内的监控市场产生影响是最困难的，因为它是一个如此庞大、自给自足的市场。

当许多技术服务器和基于云的技术仍由西方公司提供时，情况更容易。目前，中国在其监控基础设施方面已经变得非常独立，不再那么依赖西方技术。

何：量子计算——中国谈论它已经很长时间了。党和媒体认为这是中国可以超越美国的地方。但现在美国量子计算公司似乎正在取得突破。你对

中国与美国在量子计算方面竞争的评估是什么？

韦：我们也听到来自中国的突破。有论文声称已经破解了加密，无论是轻量级还是重量级加密。在一些情况下，这种观点已经被驳斥。

中国政府似乎仍在取得良好进展。它已经向量子技术和研究投资了数十亿美元，在量子通信方面一直处于世界领先地位，这是一种通过量子设备和卫星安全通信的方式。

然而，防范量子计算的另一个发展是量子密码学 (quantum cryptography)。在这个领域，我认为中国永远不会完全成功，因为他们总会有后门。他们会在量子密码系统中获得后门，如果有后门，还有什么意义 —— 如果它毕竟是不安全的技术？所以中国不会在量子计算方面达到顶峰。

中国有自主系统，但它仍在进口西方技术，这表明它需要西方技术 —— 硬件、量子计算机。我们知道中国进口了一家加拿大公司的量子计算机来进行实验的案例。

你听到的所有这些突破都很难评估，因为没有适当的量子计算基准。即使在美国，当你听到来自微软或其他公司的消息时，也很难知道。在我们有了基准之前，很难评估美国或中国的比较实力。

何：在量子领域中是否能够及时关注到技术突破？

韦：研究小组 —— 中国的学者和美国的私营公司 —— 必须发表他们的研

究。他们必须销售他们的产品或推进他们的学术生涯，所以他们有动力将其公之于众。如果有突破，我们会很快看到。

我们必须关注那个领域。有些人说比特币也会受到量子计算机的威胁，因为它们将能够解密。如果在某个时刻有大量比特币移动，可能是量子计算机已经到来，因为所有比特币都必须转移到后量子密码学 (post-quantum cryptography)。但一些比特币，特别是中本聪 (Satoshi) 持有的比特币，不太可能转移到后量子密码学。

何：你对世界赶上量子加密方法有多大信心？如果量子计算突破真的发生了，比特币不会是我们需要担心的第一件事，因为所有银行、军队、政府、公司——每个人的加密都被破坏了。你认为世界会出现这样的情况吗？

韦：许多国家已经开始向量子密码学迁移。他们从政府中最关键的系统和最敏感的数据开始。一些军队已经创建了量子安全的网络，使用量子密码学。

我认为最关键的数据将在量子计算机到来时得到保护——根据当前的评估，那是在 2030 年或 2035 年或更晚。然而，私营部门仍然远远落后。几乎没有公司为短信进行后量子密码转换。只有 Signal 和 iMessage 有，但其他的没有。目前电子邮件服务没有抗量子破译的能力。所以所有这些都容易受到量子计算机的攻击。金融数据的保护非常关键。

我们在正确的轨道上，但我们需要加快一点速度。私营部门尤其非常缓慢——他们没有看到紧迫性。

何：Signal 和 iMessage 已经量子安全了？

韦：它们已经是量子安全的。这很重要，因为中国和其他大国已经在收集他们以后能够解密的数据。目前他们还不能解密，但在 5 年或 10 年后他们可能会。具有长期重要性的数据，他们将可以访问 —— 活动人士非常敏感的数据，关于这些人的数据在 10 年或 15 年后仍然重要。

何：这件事情有多重要？

韦：我们应该非常关注，因为目前，大多数数据都在中国的触及范围之外。如果你使用端到端加密，或者即使是我们交谈时的加密，中国还无法访问它。我们需要关注中国在 10 年后仍然关注的数据。我们必须考虑那将是什么数据。

无论是活动人士还是记者，中国在那个时间框架内仍然关心什么？他们可能不太关心你今天的杂货购物或今年的位置，或者你一直在与谁交谈，但可能有其他数据他们仍然渴望了解 —— 与中国的家庭成员的联系，或者在 10 年后仍然相关的事情，他们可以用这些数据对活动人士施加压力。

何：我不知道中国政府在 10 年后会关心什么，也许它们自己也不知道。在这种不确定的情况下，党的最佳策略似乎是囤积数据 —— 尽可能多地获取并尽可能长时间地存储。

韦：是的，他们想要尽可能多的数据。

何：你能谈谈量子计算机和其供应链吗？

韦：目前，西方国家和中国的供应链仍然非常分离，这是好事。它们不依赖中国的技术，应该保持这种状态。我们不能依赖中国的量子技术。

许多重要技术在西方国家生产——欧洲、美国、日本。记住这一点非常关键，这是我们仍然在技术供应链中拥有优势的少数技术领域之一。我们必须意识到这一点。

何：你能对比一下吗？芯片也在国外制造，尽管稀土有时来自中国。

韦：稀土仍然很大程度上由中国控制。就芯片而言，中国一直在快速进步。他们在赶上西方方面取得了快速进展，我认为他们在实现独立方面比在量子技术方面做得更好。但他们仍然非常依赖西方技术，特别是对于最新的芯片，尤其是阿斯麦尔 (ASML) 和芯片生产设备。他们非常依赖高功率英伟达芯片。

很难对比这两者——量子和人工智能——因为人工智能已经更加先进，量子仍然是一个非常新生的领域。

何：数字货币——还有一个反乌托邦的功能，你支付的每一分钱都可以被国家追踪，通过数字痕迹更容易追踪。它使资助活动人士和人权工作者变得更加困难，使国家不喜欢的一切变得更加困难。我们在这方面处于什么位置？鉴于人们已经被支付宝和微信追踪，这有多重要？无论如何，你几乎不会用现金移动那么多钱。数字人民币真的有多大的增强？

韦：这是一种增强，因为它消除了国家想要的数据和公民之间的中介。目前你有银行，你有支付宝，你需要通过他们获取数据。但有了数字货币，你就可以消除那个中介，直接访问金融数据。

何：这是一种有趣的看待方式。通常当我们考虑数字货币时，我们考虑消除中间人——中介和金融机构——为了分散的、个人对财务的控制。

韦：你有分散的货币，这是中国不想要的，但你也有像数字人民币这样的集中货币。加密货币等分散货币在中国是被禁止的。数字人民币符合中共的利益，因为它对其拥有完全的控制权。

生态系统：民主、专制和公民社会

何：中国和其他专制国家用于警务的许多技术也被民主国家使用。特朗普政府现在有一个计划，用 Palantir 创建一个公民数据库，它也有面部识别和其他功能。这不是美国第一次试图开发监控基础设施。你对此有何评论？民主国家，特别是美国，面临着类似的专制数据中心、技术增强的专制主义威胁。

韦：危险是非常现实的。中国存在的许多技术在美国也存在——面部识别相机、手机跟踪器、社交媒体监控。在巴尔的摩，甚至在十年前，他们就有在战争期间部署的无人机来监视城市。所以美国正在部署这些重型和强大的监控技术。

同时，美国存在强大的民主技术生态系统。在美国，你有 Signal 等平台，

这是端到端加密的，在中国被禁止。在美国，几乎所有网站都通过 HTTPS 运行，这是保护用户免受政府监控的安全方式。在中国，很多网站没有 HTTPS。

你还有保障措施，如政府内部数据的孤岛化，尽管有些人试图打破它并创建数据融合。拥有某些数据的政府机构，还没有与另一个政府实体的数据融合。所以在美国实施专制主义存在这种困难。但政府可以慢慢地削弱它。如果持续这样做，只是时间问题，直到政府进入一个更加等同于中国的技术生态系统。

何：你有这个术语“一键式极权主义”(turnkey totalitarianism)，描述的是民主国家也可以开发所有压迫和监控的基础设施，然后当时机到来——当宣布紧急状态到来时——民主国家可以翻转开关，鉴于已经存在的能力，一夜之间变成专制。民主国家离翻转开关有多近？我们是否正在接近那个钥匙？

韦：这取决于民主国家自身，但总有一个过渡时期。在民主国家，政府不能一夜之间将民主变成专制政权。即使它拥有所有技术，它也需要改变治理结构。在民主国家有法院、议会，所有这些改变都需要时间。

但如果它只想改变技术，那会很快——使用国家拥有的技术并将其用于专制目的。那会快得多。但它必须改变机构来实施它，这需要时间。

何：在民主的光谱上，一边有中国，另一边有美国和欧洲。然后中间有许多国家，具有不同程度的民主韧性、稳定性和质量。中间的这些摇摆国家

几乎是双方的战场。中国显然试图影响这些国家变得更像他们，拥有以某种方式接近选举、活动人士和媒体的技术。在你看来，西方是否做得足够多，使摇摆国家倾向于民主？

韦：西方做得不够。我们必须做更多来占据技术空间。在过去 20 年里，我们给了中国很多技术空间。他们在国外建立了 5G 基础设施，建立了许多国家的骨干互联网，整合到中国提供的智慧城市中，然后这些都被用于专制生态系统。这是真正的危险。

我们必须更好地出口根植于我们价值观的技术。我们必须占据技术空间，特别是在摇摆国家。在很多摇摆国家，中国拥有很多技术空间，它们可以借助中国的技术自由地建立镇压能力。中国出口的技术越多，那些摇摆国家就越容易使用它们。对于西方国家，如果它们看到其中一个国家的民主倒退，它们可以潜在地限制对该国家技术的获取，但如果中国正在出口它，西方国家就没有这个杠杆。

何：那么正确的剧本是什么？你可以想象中国销售各种警察技术，而西方试图阻止这些销售，那是剧本一。剧本二，中国正在销售符合他们价值观的技术，西方应该销售符合自由西方价值观的技术。剧本三，两者都做——阻止中国销售，也销售西方技术。

韦：根据我的经验，很难阻止中国技术出口到国外。这总是一个国家的决定，而且有需求。大多数国家无论你是否想要阻止都会购买它。你不能强迫每个人不购买各种技术。

所以我们必须处理现有的情况。我们必须尝试出口更多。我们必须成为——并保持——技术领导者以继续出口。同时，我们必须支持自由技术 (freedom technologies)。我们需要加倍努力创建整个自由技术生态系统。如果中国技术已经到位，我们需要为人们提供工具来应对它，在那个敌对的技术空间中仍然保护隐私和匿名性。

我们必须假设活动人士的许多空间将是充满敌对技术的，我们必须为他们配备使其不那么危险的技术。我们必须创建这些由自由技术赋权的支持领域。开放技术基金 (Open Technology Fund) 就是一个很好的例子，这些技术正在那里得到资助和开发，但我们需要加倍努力。

何：我们应该多大程度上责怪科技公司？苹果公司在中国已经很长时间了，新书《苹果在中国》记录了苹果如何通过实践培训和数十亿美元的投资，基本上将他们的制造专业知识转移到中国。Meta 有对中国政府有力的内容审核偏见。谷歌有（已停止）蜻蜓计划 (Project Dragonfly)。西方科技公司是否过于同流合污，在世界各地，特别是在中国，迎合专制主义？

韦：他们应该受到很大的谴责。中国的防火长城是用美国砖块建造的。这是杰克·戈德史密斯 (Jack Goldsmith) 和蒂姆 (Tim Wu) 在他们的书中写的——他们发现思科 (Cisco) 提供了中国用来控制跨境互联网流量的许多服务器。正如你提到的苹果公司，还有许多其他案例。

我们应该怎么做？一种方法是公开施压，增加公众压力。另一种对抗方式是通过这些公司内部抗议——这就是当时蜻蜓计划被对抗的方式。这些是相当有价值的方式，可以推动更尊重人权的方向，而不是只看到利润。

何： 非营利组织在这个生态系统中的作用是什么？你提到了开放技术基金，还有公民实验室 (Citizen Lab)、Access Now。非营利组织如何有效地对抗数据中心型专制主义？他们需要什么才能有力挑战这个非常强大的国家和企业利益联盟？

韦： 他们都在各自做着出色的工作。公民实验室揭露了针对活动人士的全球间谍行动。开放技术基金开发了许多帮助活动人士的技术。Access Now 追踪互联网关闭。我们有 Signal，我们有 VPN，但人们还需要什么其他技术？例如，一个保护隐私的 ChatGPT —— 可以设想这样的事情。

但我认为还没有一个关于如何建立民主技术生态系统的总体战略。当各方面聚合到一起时，可以提供一个非常强大的共同制定战略的方式。它在正确的轨道上，但也许可以有更多的协调。

我仍然认为在对抗数字专制主义的实体和对抗专制主义的实体之间存在分歧。有些组织试图推动密码学研究，其他组织则建立数字工具，但我认为我们需要更好地整合这两者 —— 那些关注线下世界的非政府组织和那些关注在线世界的非政府组织。

何： 如果以不同的方式使用，我们谈到的技术实际上能增强自由吗？我们谈到了神经技术、数字货币、人工智能监控和量子。民间社会是否有可能利用这些技术作为自己的优势？

韦： 这是可能的，特别是当它们容易获得时。我们知道，在学术界，有很多研究人员正在研究为更好的目的开发技术。它绝对可以用于善。人工智

能可以用于民间社会，特别是当它是开源的，当他们可以修改它并为自己的目的开发它的时候。

对大多数人来说最适用的情况是人工智能，因为目前对于神经技术、量子数字货币，我看不到有很多机会改变它，使其向自己的优势倾斜。

何：就实际指导而言，我们谈到了 iMessage 和 Signal 是量子安全的，所以我想这些将是你今天向中国民主活动人士推荐的。

韦：对于海外的中国民主活动人士，有一整套他们可以使用的工具和基本的网络安全措施。双重身份验证非常重要，以及 Signal 和值得信赖的 VPN——有很多 VPN 是由中国政府赞助或批准的，所以我们必须小心不要使用那些。

每当使用中国生态系统时——无论是 TikTok、微信还是支付宝——都必须假设该信息已被泄露。所以要总是以假设信息被泄露的方式使用它。

何：人们是否有特定的地方可以发现这些数字自由技术？

韦：有一个叫做安全规划师 (Security Planner) 的工具。如威胁来自国家行为者，你可以根据你的威胁模型进行编辑。可以添加你正在使用的设备——PC 或手机——你关心什么，然后你会得到关于如何减少与技术 and 该威胁模型相关的安全风险的建议。这是最好的方式。

但如果你在互联网自由社区，最好的方式就是继续与你领域的其他组织交

谈并交换知识，特别是与公民实验室、Access Now(现在接触)、人权观察 (Human Rights Watch) 等组织的研究人员。

何：这是一个很好的观点。iMessage、WhatsApp 和安全规划师是人们可以采取的个人层面的行动。活动人士如何建立更有韧性的集体网络，既有效又安全？你有可能感兴趣的成功模型吗？

韦：对我来说，最有效的是该领域的人员和研究人员的个人网络，在互联网自由社区，特别是那些你可以在互联网自由聚会上见面的人。这是最深刻的，因为你可以提问，交换经验。这对我来说真的是获得定制安全建议和交换安全实践的最有力方式。

何：展望未来，你认为未来五年的前两个优先行动是什么？

韦：一是，正如我之前所说，我们需要为互联网自由工具和技术提供更多实质性和可持续的资金，无论是在美国还是在欧洲。我们需要扩大这一点。

其次，我们需要赋权国际社群，更主动地与摇摆国家、混合政权中的议员接触——特别是关心人权的反对党议员。我们需要与他们就中国监控项目进行接触，看看如何对抗这些项目，特别是在地缘框架中。将来自一个地区的不同议员聚集在一起，就如何推动反对中国监控影响力进行战略规划，这可能真的很有力。

第三，追踪中国监控项目和信息控制项目在海外的情况真的很重要。这就是为什么我们需要强大的地方媒体，它们可以批判性地和独立地报道这些。

正如我之前提到的，我们需要整合在线部分 —— 技术部分 —— 与赋权世界各地的地方行动者的线下部分，以跟踪技术并在议会和其他地方对抗它。

何： 是否有记者和研究人员一直未能提出你认为真正重要的问题？

韦： 关心在线权利的人权社区和更广泛地关心专制主义的人权社区之间存在分歧，我们需要弥合这种分歧。

老实说，我认为我们对中国的关注太少，我们对中国内部的专制主义了解太少。更好地监测那里正在开发的技术真的会有帮助，以了解我们很快将面临什么。这将帮助我们领先中国一步 —— 已经知道什么会影响我们。我们可以领先于很快会影响我们的事情。我们需要更好地监测中国内部的监控技术，并看看我们如何在未来对抗它们。

何： 最后一个问题 —— 鉴于你研究的技术能力、出口、企业复杂性 —— 你是否对民主的数字未来抱有希望？你对未来和反击威权统治的前景感到乐观吗？

韦： 我非常乐观，因为威权领导人总是表现出有力量的形象 —— 然而每个威权领导人最终都是非常软弱的。他们对政权安全有恐惧，这就是为什么中国在监控技术上投入如此之多 —— 因为他们感到非常脆弱。变化将会发生在最意想不到的时刻。

谁会在八十年代中期想到苏联会崩溃？柏林墙会倒塌？同样，现在中国可能感觉非常稳定，那里的政权是安全的，但事情可能会很快改变。我们在

新冠大流行期间看到了这一点，中共政权受到了相当深刻的动摇。

我认为还会有更多这样的时刻到来。这就是给我希望的东西。威权领导人最终不是好的统治者。他们不是好的决策者。他们在误判。

何：感谢你接受我的采访。

注释

- 1 报告链接：https://www.ned.org/wp-content/uploads/2025/02/NED_FORUM-China-Emerging-Technologies-Report.pdf
- 2 人工通用智能 (AGI, Artificial General Intelligence), 是一个不局限于单一任务的“总体式智能”系统，其能力将在所有领域、所有认知任务中与人类相媲美或超越人类。