# 中国和俄罗斯信息控制的全球网

Valentin Weber

Research Affiliate, Centre for Technology and Global Affairs, University of Oxford
Information Controls Fellow, Open Technology Fund

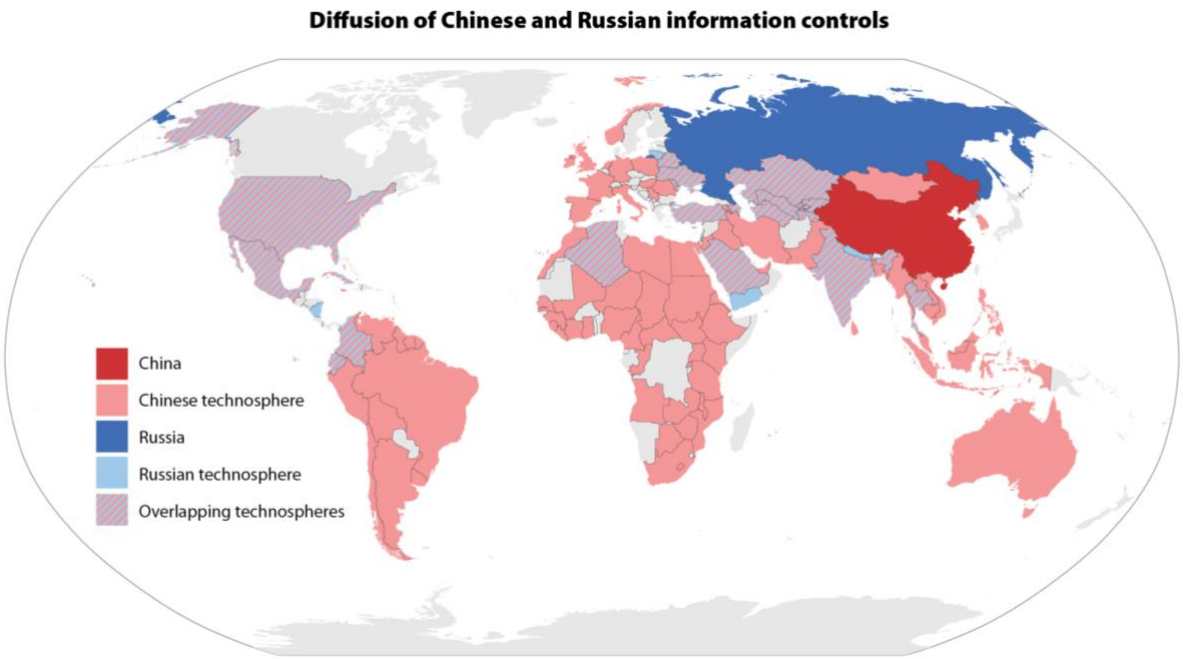
## 摘要

中国和俄罗斯信息控制的科技和技术在全球扩散已经成为主要国际报纸的显著标题。然而，对此种扩散的驱动力以及结果却鲜有系统性的分析报导。本文针对此一题目研究发现，这两国的信息控制正更有效地扩散至混合式或威权国家，尤其是那些与中俄有关系的国家。中国的信息控制较易于扩散到其“一带一路”沿线的国家；俄罗斯之控制散布于独联体各国。在研究得出此一结论过程中，本文首先定义出俄罗斯和中国的信息控制模式，然后追踪这两国的信息控制在其各自的「科技圈」(technosphere)所及共 110 个国家中的扩散，这指的既是地理区域，也是中国与俄罗斯信息控制科技、信息处理技术以及法律扩散所及的影响范围。

## 前言

北京和莫斯科的信息控制科技 (例如，出口审查设备、安全城市)、和技术(例如，由其他国家模仿中／俄监视法律)已走向全球，其影响既扩及加勒比地区仅有 8 万或 10 万居民的小岛国家，如安提瓜和巴布达，也到达人口超过 10 亿的南亚国家（印度）。来自巴哈马，莱索托和秘鲁的记者参加了在北京的宣传培训，中国的监视装备已经用在巴西东部的军事指挥部，以及约旦的议会大厦。俄罗斯的监视设备部署在其邻国，如白俄罗斯、哈萨克斯坦、和乌克兰，也部署在遥远的阿尔及利亚、古巴、墨西哥、和巴勒斯坦。

研究此类重大扩散之时，很重要的一点就是了解，为什么俄罗斯的信息控制，而非中国的信息控制，能在一些国家扩散，而非别的国家。什么促使这种控制能在不同地区扩散？如果在一个国家中扩散的是某一套控制，而非另一套，差别为何？这种国际繁衍如何使这两国受益匪浅？




**地图 1:**俄罗斯与中国信息控制的扩散。

为了回答上述问题，本文首先建立了信息控制类型学。第二节即引用信息控制类型，检视俄罗斯和中国信息控制的做法。第三节揭示如何测量扩散，第四节说明扩散的原因。第五节追踪和分析中国与俄罗斯的此类科技，包括技术与法律的模仿以及培训，在国际上如何扩散。本文第六节明确指出中国和俄罗斯因信息控制出口而获得的政治、经济和情报优势，以及这种扩散对进口国的影响。本文的结论也提出一些建议给民主国家，如何在未来削弱信息控制科技潜在的滥用。

## 1. 信息控制类型学

对信息控制的定义，学者间意见殊异。一些学者指出，信息控制的概念为“在网络空间内且通过网络空间进行的行动，以寻求阻绝、中断、操纵和塑造信息和通信，达到战略和政治目的。”另外一些学者将信息控制分类为恐惧(即，自我审查)、摩擦(类似审查)、和泛滥(近似战络信息散发)。有别于这些学说，本文认定信息控制的核心概念为“监视”(surveillance)，并分析如何藉监视影响管理信息的其他形式。信息控制可以有不同形式：包括监视、审查(censorship)、自我审查(self-censorship)、和战略信息散发(strategic information dissemination)。当虑及一个国家使用各种各样信息控制形式的程度，并评估其控制信息的选项(工具)数量，即可呈现形形色色的信息控制模式。

## 监视(surveillance)

要对信息控制有全盘概念，监视至关紧要。有了监视，才可以进而做到审查、自我审查、和战略信息散发。没有监视就没有威吓，而政府也不知道要阻绝哪些网站，当局也无从知晓哪些网络对话需要接受“政治指导”。

监视可被观察出来，也可能没被观察到。当一般民众查觉有监视时，就会引起人们的自我审查。很明显的，展现出有监视可以不必实际进行监视，就能有监视之效。一个政府可能安装假相机，就可以吓到市民。即使监视不被民众查觉，它仍然产生影响。当监视未被察觉时，依旧可以用来阻挡特定内容(审查)，或指向特定目标散发战略信息。

如对监视略而不提，探讨信息控制的任何理论都不完整。过分关注内容和网上发生的事情(如，关键词过滤)，就无视于科技对网络外世界的重大影响(如，以监视摄像机进行实体监控)。近年来，网络世界(在线)已与实体世界(离线)合而为一。数码 1 与 0、位和字节定义了所有日常事物。在一个世界中，当闭路电视摄像头、智能城市、和其他网络暨实体系统无所不在时，信息控制就越来越成为实体控制。网络安全专家布鲁斯·施奈尔(Bruce Schneier)言简意赅的指出：“互联网不再是我们连上的网络。相反，这是一个计算器化、网络化、互联化的世界，而我们身处其中。这就是未来，我们称之为物联网。”汽车现在是各种计算器的一个组合，再配上铁皮与轮胎，而日常的工具现已附加了监视工具包。举例而言，中国的汽车制造商把电动车的实时位置和其他信息传输给政府。在今日中国，电动汽车可以是监视的工具，而这些车变为实体控制工具只是时间上的问题。因为网络世界和脱机世界已经如此紧密融合，一个人在网上所说、所写、所听的内容，与他每日的“做为”紧密交织而不可分，即使这些刚刚做的事原本可以当成跟网络没有关系。

## 自我审查(self-censorship)

“自我审查”起自于担忧法律和法外(威吓)的处罚，以及恐惧将来会出现对个人／实体单位的监视（例如，被当局当成“不从众者”(non-conformist)）。虽然恐惧感可能是推动自我审查的主要因素之一，但并非每一次自我审查的行为都伴有恐惧感。“当一个人面对着可能有潜在敌意的说话对象时，有很多原因会使这个人保留自己的意见，比如可能是想避免口角之争，或担心冒犯了别人或伤了别人的心，或担心受到报复，如丢掉工作、或有被打的危险，或担心被当成异类。”有鉴于此，本文仅定义“自我审查”为“以为听我说话的对方会跟自己的真实

意见相左时，就保留自己的意见。”一个政府手中可任意运用的监视工具越多，就越容易驱使民众走向自我约束。

**审查(censorship)**

审查是一种“他人压制某种观点的传播，当这种观点被这些他人视为有敌意或具挑战意图”，而审查可经由不同方式进行，有时是很细微的做法，如使取得信息的成本提高了，或把某些网络服务降速(如 Tor)，或把不妥的政治内容在搜索引擎中降序。审查也可能是大规模、无差别的做法，如关闭某些社交媒体平台、手机服务、或中断网络联机。

依监视能力，审查可以变化。更多元化的监视能力代表有更多选项可以用来执行审查。一个不太高明的政府想限制信息，可能只有采用网络封锁。相较之下，手段复杂的政府可能会选择把关键内容降级，让信息难以取得。

**战略信息散发(strategic information dissemination)**

战略信息散发意谓着政府在战略层面，利用“宣传”和“虚假信息”，操纵公众舆论。此处“宣传”一词指“公开散发信息，以影响他人的想法和／或其行动”，而“虚假信息”(disinformation)通常的理解是“基于恶毒意图，蓄意散播的错误信息”。就本文讨论范围，虚假信息的例子之一就是，俄罗斯假造“新闻”：艾滋病是美国政府实验的结果，并大肆传播。而宣传的一个例子就是中国政府运用“微博”账号，通常这些账号是用来分享照片、影片、与文字的。一个受欢迎的微博平台是新浪微博(Sina Weibo)。战略信息散布跟审查一样，可以依传播者的监视能力而有变化。一个国家对其人民知道的越多，操纵人民的选项就越多。

**使用程度**

形形色色信息控制的使用程度经常取决于许多具体情境因素。各国在某种程度上都受限于能掌握的工具。例如，比起中国，俄罗斯想实施严格网上审查制度的选项较少，因为其互联网科技的监控基础设施较不完备。因此，俄罗斯主要是借着威吓人民(例如，监禁反对派候选人)，以及透过宣传与虚假消息散发来操纵人民。俄罗斯仰赖这些技术，可能是因为这些做法不需要太复杂的科技。

**选项**

一个国家的监视能力，界定了统治当局进行信息控制时可有的选项数目。例如，使用间谍软件渗透手机的某一国家可能藉读取某些信息，用以恐吓反对派人士。然而，一个国家如果没有深度封包检测工具(用来网络过滤与监视)，即无法取得其他信息，因此就限制了这个国家设定其他目标异议分子的能力。更高的监视能力并不一定能转成更有效的信息控制，但当局如果拥有复杂的监控技术，即能有多样的工具箱，以选择执行信息控制。因此，将监视纳入信息控制类型，可对不同国家的信息控制做出更扎实的比较。例如，中国拥有比俄罗斯更高的监视能力，因此有更多选项来实施信息控制，这将在下一节深入讨论。因此，监视工具的数量和多样性是理解中国和俄罗斯信息控制模式各自特色的一个主要因素。

监视、自我审查、审查、和战略信息散发共同构成了信息控制的机制与形式。一个国家依赖每种机制的强度，结合它实施每种机制的选项数目，界定了该国的信息控制模式。

下节显示，俄罗斯仰赖遍布式的监视、自我审查、和战略信息散发，以维系国内稳定，而中国以广泛的监视为基础，大规模使用审查和战略信息散发。中国与俄罗斯两种模式有重迭之处。中国在某种程度上与俄罗斯一样，以法律规定网络平台实名注册制，以及把 VPN 拥有者关进牢里，进而驱使自我审查。俄罗斯也与中国一样，订出禁用网站黑名单，实施审查制度。

## 2. 中国与俄罗斯信息控制模型

在比较俄罗斯和中国的信息控制模式时，一种有效的方式就是检视他们依赖各种机制到何程度，以及各自能支配哪些工具，以实施控制。

### 俄罗斯的做法

#### 监视

俄罗斯 1995 年的“行动调查法”(Law on Operational Investigation)为实现广泛的监视框架建立了法源，该法允许“俄罗斯联邦安全局”(Federal Security Service of the Russian Federation，FSB)实施网络监控“行动调查活动系统”(System for Operative Investigative Activities)，简称为 SORM。SORM-1 专门用在拦截电话与手机通话。为因应互联网普及率的飙升，就成立了 SORM-2，监视互联网流量。之后，SORM-3 提升与增加了当时监视系统的功能，如监看社交媒体和 Wi-Fi。

## 自我审查

在 2000 年早期，新的“俄罗斯联邦的信息安全准则”(Information Security Doctrine of the Russian Federation)出台，将信息安全界定为国家安全事务。随后，多项限制跟进，如 2014 年的“博客法”(blogger's law)与“反加密法”(anti-encryption law)，及 2016 年的一项立法，规定数据存储需本地化存于俄罗斯境内。这些法律足以展示俄罗斯对其人民遍布式的监视，并促使自我审查。

同时，俄罗斯当局威吓艺术家、新闻记者、科技主管、和反对派代表人士。反对派的 Boris Nemtsov 被杀，政治行动者 Alexei Navalny 多次入狱，而 VK 电报信使(VK and Telegram Messenger)的创办人 Pavel Durov 在政府持续高压下，只得流亡。更微细的恐吓措施也产生了深远的影响。俄罗斯国家主导的全国性的公示，不断强调互联网的危险，经研究发现，这也导致自我审查增高。

## 战略信息散发

在俄罗斯，宣传与虚假信息的重点是发送有利于政权的信息。学者 Gallagher 与 Fredheim 指出，“互联网研究机构”(Internet Research Agency) 是个俄罗斯编造厂，对国内，就是统一言论口径，在国外，就是制造分裂话语。从 Twitter 上发给国内民众的消息就是强调应该支持俄罗斯介入乌克兰和叙利亚，并夸大西方阵营的分歧。俄罗斯编造厂散发讯息时，有时也会走官方媒体频道，如 Channel One、Russia One、NTV、Komsomolskaya Pravda、与 Izvestia。这些动作有助于扩大克里姆林宫战略信息的散发范围。“互联网研究机构”付费的博主，和另一个宣传组织 *Nashi* 青年运动的付费博主，主要是由秘密雇用的民众组成。其中有些人全职工作，以 12 小时为一班上班。

## 审查制度

俄罗斯政府一直都较不重视审查制度。跟中国不同的是，俄罗斯一直未能建立可以替代外国媒体平台的本国平台。而俄罗斯的科技公司，包括本国人经营的 app 应用程序商店、搜索引擎、或社交媒体平台等，都未能有足够的国内市占率，可以排除或取代外国竞争者。此外，俄罗斯的网络过滤采用了一个全国性阻挡清单(blocklist)，并使用深度封包检测工具等其他先进技术，维持高度监视。但是，俄罗斯过滤的遍布程度不若中国。例如，Alexei Navalny 经常抨击政府，但他的 YouTube 频道仍在营运。

最近，俄罗斯进一步严打网络环境，试图封锁 Telegram Messenger，但是政府封锁方法太粗糙，导致俄罗斯大片互联网停摆。所以，Telegram Messenger 仍然在应用程序商店可以取得，政府如果想封锁，技术设备远远不足。这显示俄罗斯在封锁技术与手段上不如中国复杂，中国实施的审查更为滴水不漏、隐蔽无踪。俄罗斯在 2017 年还通过了一项法律修正案，限制 VPN 的使用。但是即便有了这些新法规，仍有一大堆翻墙 apps 在 Apple App Store 和 Google Play Store 可以获得。

## 中国的做法

### 监视

与俄罗斯相比，中国在监视民众时，有更多的选项，因为监视装置已经遍布现今的中国社会。举例而言，在新疆，当地人受到无所不在的监看，监视系统结合了侵入式应用程序、面部识别摄像头、和其他技术。监视设备已经布建全面，深入社会。这在中国的教育体系内也处处可见，学生在教室上课，由教室中的面部识别系统监看，学生到哪里都可透过手环追踪，上面记录他们的地理位置。虽然这类监看是由学校执行的，但这是政府的“智能教育”计划所支持布建的。

政府也有各种方案，鼓励监视大军中的民间参与者推动民众进行自我审查，这些民间参与者就在政府的监视努力中扮演了补强的角色。研究发现，经常暴露于监视中，会促使一般人自我审查。中国已经有如此广泛的监视系统，可以预期会出现类似的效应。

### 审查

在中国，最明显的审查事例就是其防火墙(Great Firewall)，它禁止中国人民上 Google、Facebook、与 Twitter。在中国境内，政府内部和私营公司有数以千计的审查员，在大流量信息中筛选出新的关键词设定禁用。其中大部分的审查仍然是人工操作，但有一部分筛选工作已经是自动化过滤，如使用已知关键词阻挡(known-keyword blocking)。学者 Ray Bradbury 在《华氏 451》(*Fahrenheit 451*)一书中提出的大哉问又可再次提出，“你烧了的书中，你曾经读过其中任何一本吗？”换言之，审查员真的读了他们审查掉的内容吗？在未来，他们可能连读都不必，因为大部分过滤都可由人工智能自动化处理了。最近，中国甚至对那些试图连上外国网站的精英与热衷科技的公民加大审查。还有一些法规出台，使

政府不批准的 VPN 在 app 商店下架，导致在中国 Apple App Store 与腾讯 App Store 这两个主要应用程序商店可以取得的 VPN 极其有限。

## 战略信息散发

中国与俄罗斯一样，战略信息散发的重要角色之一就是为政府策略性的把敏感政治议题转移焦点。在中国，这种操作的目的是不加入争议性的话题，而是把争议的焦点从争议移转到亲政府的贴文。早在 2004 年，中国当局已经雇人来摇摆网络上的民意。他们认知到，只做到决定哪些信息可以提供是不够的，形塑仍留在网络上的信息同样重要。为此，当局聘用了数以千计的互联网评论员，专门做贴文，俗称为五毛党。据估计，网络上这样的佣兵现在高达 200 万名，每年制造约 4.5 亿个贴文。

俄罗斯和中国的战略信息散发做法有雷同之处，两者都贴发亲政府简讯，转移争议性话题的讨论焦点，也不加入政治议题的实质性讨论。五毛党似乎主要由政府员工组成，工作之余做贴文，另外还有志愿者加入，例如共产党的青年党员，他们组成“网络文明志愿行动”，无薪转发爱国内容。

## 自我审查

中国在毛泽东时代，以恐吓逼使自我审查是一种非常普遍的做法。之后，这种做法转为以审查和战略信息散发为主的信息控制方式。目前，政府针对精英阶层培养自我审查，而用审查和战略信息散发对付一般民众(这种策略控制普通民众最为有效)。诱使自我审查措施的一个例子是逮捕提供 VPN 服务的人(作为对其他 VPN 供货商的警告)，或者强制规定社交媒体上有影响力者必须实名登记。除此之外，为鼓励自我审查，中国的互联网法律往往故意规范模糊，在该罚与不罚间制造模棱两可的空间。

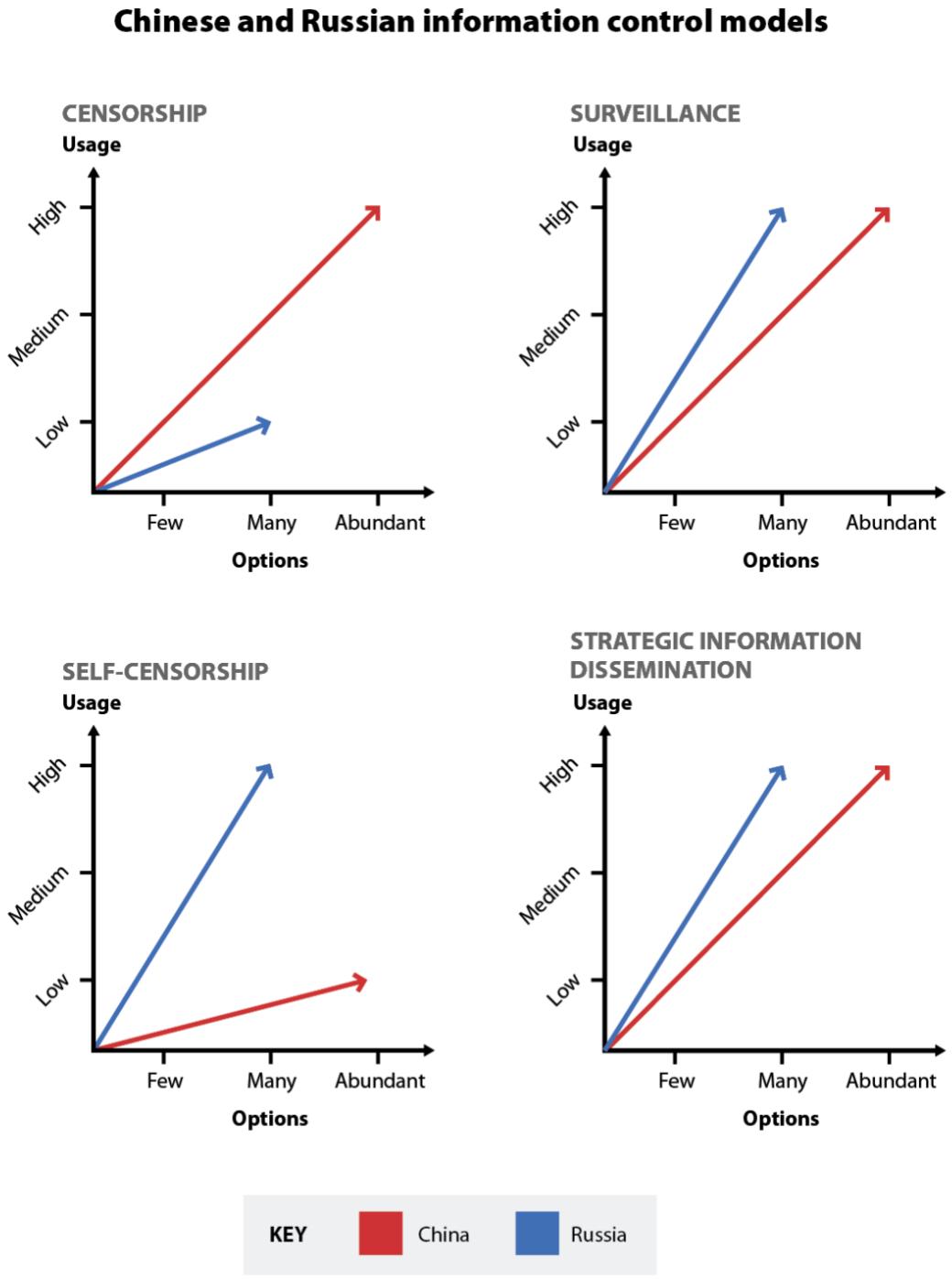



**图 1-4**：中国与俄罗斯信息控制模式。

## 3. 研究方法：测量扩散

针对中国与俄罗斯信息控制科技与技术的扩散，本文的研究方法是开放来源追踪法，分析从公司报告、技术网络测量、报纸或期刊文章、以及政府法规中收集的数据资料。

本研究以三个指标来衡量扩散：科技、模仿、与培训。用这三个指标的目的是衡量中国与俄罗斯对其他国家运用的战术分布所及的广度和深度。广度指的是有多少国家暴露在至少一个指标之下。深度指的是单一国家采用了几个指标。如果一个国家采用了一项扩散指标，就定位在“科技圈”的外缘。如果一个国家被标上最多指标(俄罗斯的两个指标，中国的三个指标)，则在这一国的扩散就被视为深广，该国就落在“科技圈”的中心。

**指标 1：科技**

扩散的第一个指标是科技。就本文的研究目的，我的焦点是放在中国与俄罗斯的监视和审查科技出口到海外实体，这些外国对象可控制大量的人口或公共建筑，可以假设是由警察或其他政府主管单位经营。此类科技的实例包括安装在监狱、港口、城市、火车站、机场中的摄像机，以及由海外互联网服务供货商部署的过滤设备。此一指针不包括监视系统出口给非警察或非政府单位，如海康威视出口给日本一间公立大学的闭路电视。

除了阅览公司声明和媒体报导，进行追踪监视出口项目外，我与 Vasilis Ververis、Nguyen Phong Hoang、以及 Marios Isaakidis 合作，透过网络测量，辨识出一组特定的监视中间箱。我们使用 OONI Explorer 和 Censys，来寻找有“V2R2C00-IAE/1.0” 指纹的华为中间盒。这个指纹或标头出现在华为的 eSight 产品，这个对象能够分析网络流量以及发现 IpSec VPN 服务 -- 这就可以用来监控和审查流量。在检视了 OONI Explorer 和 Censys 的数据后，显示出华为中间盒已经用在哥伦比亚、古巴、意大利、墨西哥、尼日利亚、巴基斯坦、西班牙和土耳其。

**指标 2：模仿**

就本文的研究目的，模仿的定义为：另一个国家复制中国或俄罗斯的信息控制法律和技术。例子之一是乌兹别克斯坦仿效俄罗斯的国家监督法；而坦桑尼亚和津巴布韦政府官员宣布，他们打算模仿中国用本土的内容提供商取代外国网络内容提供商，以强化控制。本文收集的数据显示，如果没有同时配合科技和培训的扩散，模仿几乎不会单独发生，但科技和培训扩散指标可以单独存在。

因此，模仿显示深度扩散。很显然，所有模仿俄罗斯或中国的国家即处于其各自“科技圈”的核心。

**指标 3：培训**

此一指标包含两类培训：一、对执法人员、政府官员、以及私营公司(经常为政府实施信息控制的公司)的培训，二、对新闻记者的培训。对第一类对象，就是教他们如何扩大搜取有关民众的信息(数字取证、安全城市项目)，或如何更有效地实施审查。所有智能城市的落实或销售深度封包检测技术都几乎一定配有相关技术操作培训。本文仅纳入有书面文件明文提到向特定国家提供培训的案例。举例而言，一宗只报导了华为在西班牙建设一个安全城市的新闻，即不纳入此一培训指标。

而第二类，即在中国培训海外记者，可能各国政府都没有注意到，因为其中一些培训是由私人机构或新闻机构举办。此类培训旨在增加海外对中国的正面报导。许多案例显示，这种培训达到了预期的政治效果。

“培训”一词易被误解。在西方世界，这个字的意思是：将某人提升到一定标准的熟练度，很可能是某种学术水平。然而，在中国，媒体培训实际上是公共关系目的的免费到中国参访，行程安排都是亲政府议程。..... 这种对媒体的安排，实为中国软实力战略的核心。因此，中国计划在未来几年内“培训”数百名拉丁美洲记者，最佳的解读应该是，让有影响力的意见领袖暴露在北京宣传之下的一种做法。”

此外，记者培训通常包含亲身体验信息控制方法的实际运作方式。由广西的共产党人事部门运营的广西“百色干部学院”(Baise Leadership Academy)就是一个旗舰范例，对来自东南亚的官员和记者的培训，就是教他们如何在网上“引导民意”。

## 4. 信息控制扩散的原因

本节将提供信息控制扩散的实证数据，并分析为什么相较之下，某些国家更易于模仿、购买技术、或接受培训。根据附录 A 中的实证数据，本文主张，一国的政府体制以及国与国之间的相互关联度可以解释，为什么信息控制扩散在某些情况中较易发生。

**解释变量 1: 政权体制类型**

在追踪扩散指标时，政权类型是模仿的一个主要变量，但对科技与培训的解释力较弱。本文中政权类型的定义是依据经济学人信息部(Economist Intelligence Unit)的民主指数(*Democracy Index*)，分成“民主制”(democracy)、“混合制政权”(hybrid regime)、和“威权式政权”(authoritarian regime)。本研究收集的数据显示，威权式政权和混合制更适于模仿俄罗斯和中国。在模仿中国或俄罗斯的 19 个国家中(包括俄罗斯与中国相互模仿)，58%是威权式政权，37%是混合制，仅有 5%是民主制。

为什么混合制和威权式政权更可能模仿中国和俄罗斯？理由之一或许是独裁国家间倾向更愿意相互学习，因为彼此都面临着类似的生存威胁。这种倾向使独裁者分享各种科技与政策。早在 1848 年，不同政体的独裁主政者就相互讨论和彼此分享如何对付在欧洲的革命趋势。异曲同工，在 2010 代初期的“阿拉伯之春”盛行之后，独裁者就参与了“精英学习”，让他们更了解如何塑造更充分的政策。有些状况下，独裁者之间的互助十分微细，如交换知识，但有时是明目张胆、无所忌讳的。在 2011 年有一例，就是沙特阿拉伯积极帮助巴林镇压异议人士。

政权类型对于科技与培训这两个指标的解释力较弱。虽然混合制与威权式政权占所有引进中国和俄罗斯信息控制国家的大多数(56%)，但非全部。民主国家也会购买科技或接受培训，占这两国信息控制扩散所及国家中的 37%。或许这是因为监视技术可以被民主国家用到视为“合法”的用途上，因此与民主价值观兼容。同样的，跟中国培训数字取证或新闻报导，不一定会被当成必定损及民主价值观。

此外，许多进口的科技在本质上为军民两用。例如，阿根廷、巴西、法国、德国、意大利、西班牙等民主国家进口了监视技术，而用在“智慧城市”防制街头犯罪。当然，此一技术本身可能被滥用到防止示威群众聚集。

虽然普遍认为，民主国家不会滥用监视设备，但滥用的可能性确实存在。首先，精密的监视科技总是会产生让人忧虑的理由。在民主国家，威权和非自由的措施也比比皆是。显而易见的例子，包括特朗普总统主政下的美国，维克多总理主政的匈牙利，或杜特尔特总统主政的菲律宾。其次，科技偏见会导致意外误用也是层出不穷。例如，加利福尼亚州执法机构曾经向微软提出一个要求，为警员穿的制服与警车摄像头提供面部识别功能，但是微软拒绝了，因为这个技术算法的仿真训练对象群组中绝大多数是男性与白人，所以担心其技术在处理少数族群时会不公正。

澳大利亚、印度尼西亚、英国和美国等其他民主国家的人民也都参与了中国不同单位的各种培训。例如，英国派遣人员到美亚柏科(Meiya Pico)公司，参与数字取证方法的培训，而美国和澳大利亚的记者也到中国参加学习之旅。

**解释变量 2: 互联度(interconnectedness)**

政治实体之间的双边经济、政治、历史和社会的相互关联可以解释为什么中国和俄罗斯的信息控制更易于扩散到某些国家，而非其他国家。中俄与另一个国家之间的相互联系程度越强，信息控制传到对方的可能性就越大。此一发现有别于、但是类似于学者 Levitsky 和 Way 所提出的“联系”(linkage)概念。两位学者研究在后冷战后期，西方国家与某些威权倾向政权间的关系，检视关系中所谓“联系”的概念，因而提出民主措施扩散的一项假设：扩散是建立于国与国之间关系密度的基础之上。他们发现，当“高度联系”存在，民主化即更有可能会发生。学者 Ambrosio 与 Weyland 也思考“联系”和地理邻近是与威权扩散情境的两项因素。本文的论点以这些学者的研究为基础，但在关键领域，提出相当差异的论点。

例如，Levitsky 和 Way 主张，国与国间建立紧密关系的最重要因素是地理邻近性。然而，中国与国外的互联性却延伸的愈来愈远 --可能部分原因在于该国的经济崛起。海外融资是一个可以说明的实例。从中国对不同地区的官方融资列表可以显示，非洲位居首位，其次是中欧和东欧(包括俄罗斯)，以及拉丁美洲。这些地区之后，名单上才出现南亚、东南亚、中亚和东北亚。本文提出信息控制扩散的数据也描述了同一趋势。虽然俄罗斯的信息控制已经深入扩散到独联体中的数国，但俄罗斯信息控制所扩散到的其他许多国家并非其邻国。中国的信息控制在全世界扩散既深且广，因此削弱了“地理邻近是建立相互联系，因而促使推动信息控制扩散的最强因素”此一假设。

Levitsky 和 Way 继续指出，杠杆“或政府对外部民主化压力的脆弱程度”可以解释一个国家政策和措施的变化。有鉴于此，在信息控制扩散过程中，可以想象，民主政府会迫使各国不要进口信息控制。因为信息控制科技本质上是军民两用，而且宣传培训是藉媒体培训之名，当民主国家批评这种出口之时，不被当成虚伪有些不太可能。毕竟，民主国家本身也是同类产品的主要出口国，也接受中国信息控制培训。此外，可以想象，中国和俄罗斯运用各种杠杆，使别国进口其信息控制，但中国和俄罗斯如何使用这种杠杆，做到让别国采用这些技术，在本文的研究过程中未能观察到。最后，附录 A 中所列的数据显示，扩散

的主要原因不太可能是杠杆作用，亦即，透过制裁、军事威胁、或撤出外援这种外部压力。相反，对这种设备和技术有明确需求才是更为合理的假设。

因此，本文提出了“互联度”一词，以阐述信息控制国际扩散背后的原因。本文一并探讨解释变量和政体类型变量(如上所述)，以评估信息控制扩散的可能性(见表 1)。

| | 俄罗斯／中国 | 俄罗斯／中国 | 俄罗斯／中国 |
|---|---|---|---|
| 解释变量 | 互联度 | 政权体制／互联度 | 互联度 |
| 扩散指标 | 过滤或监视科技 | 模仿法律与技术 | 培训政府与执法官员或私营公司，或新闻记者，以分享技术 |
| 扩散的深度与广度<br><br>国家 X<br>C(1), R (2) | “国家 X”扩散广度 以及扩散深度 C(1) R(2)如左栏 | | |

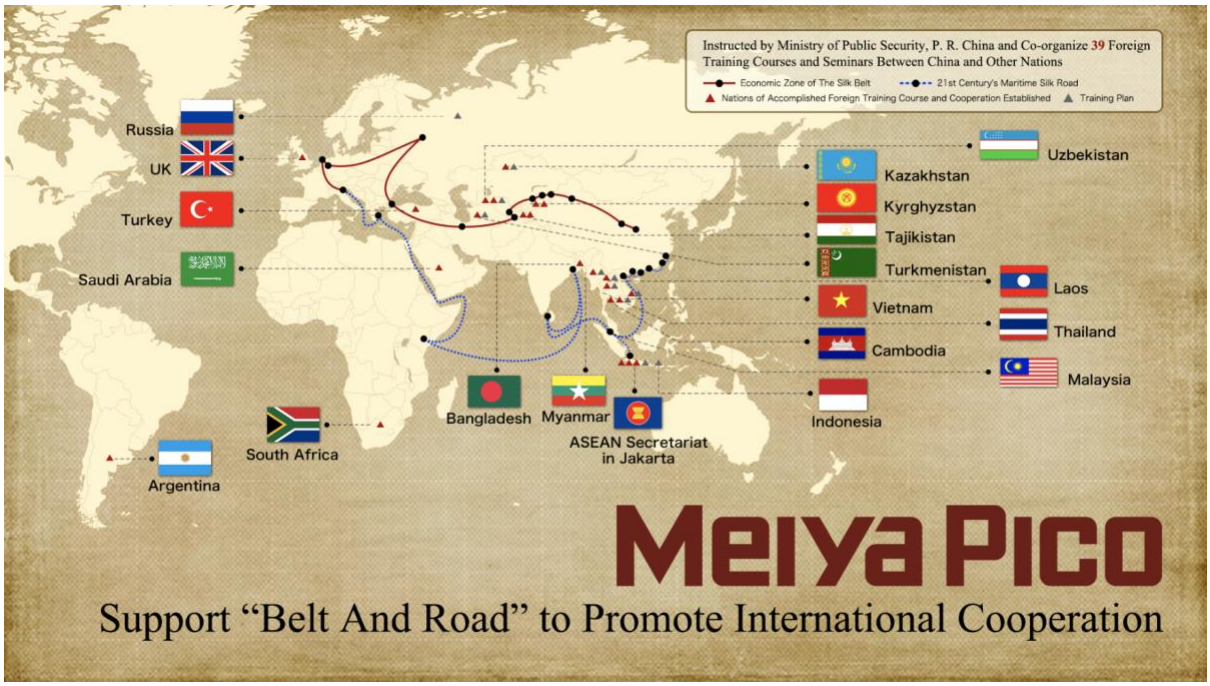
**表 1:**量测扩散

## 互联度的替代

在本文中，“一带一路倡议”(Belt and Road Initiative, BRI)和独联体(CIS)也当成显示与中国和俄罗斯有高度互联度的另一种量测替代项。就这个倡议或组织，参与其一或都参与的国家更有可能使用中国或俄罗斯信息控制。之所以如此，是因为一方面，“一带一路”和独联体基本上是中国和俄罗斯间实质经济、外交、技术官僚、社会、信息和民间社会关系的替代项，以及另一方面，这是其他参与国家之间这些关系的替代项。许多因素促成了这种对照。第一、这两个倡议都可以上溯到历史记载，中俄在古早时期与其他国家曾有紧密的互联度。“一带一路”奠基在古代丝路的复兴。另一方面，独联体植基于前苏联的传统，力图庚续旧张。其次，对这两项计划，俄罗斯和中国都积极投入。俄罗斯经常拉拢东欧和中亚，视其为势力范围之内，而中国鼓励“一带一路”沿线各国交换思想、物品、和社会互动(这些互动都在双边谅解备忘录中明文推崇)。在“一带一路”框架中，中国还把记者和媒体培训编了进去，科技和服务的销售也一并纳入。在一方面，中国企业力图寻找新的出口市场与利润。另一方面，对外贸易在一定程度上是配合政府的协调。美亚柏科是中国一家网络安全公司，接受中国公安部的指示，培训“一带一路”相关国家数字取证(见影像 2)。美亚柏科也部分参与了建立从中国到欧洲的“安全走廊”(Safety Corridor)，旨在把国安服务与产品并入国

际发展项目之中。“安全走廊”目前计划覆盖哈萨克斯坦、俄罗斯、白俄罗斯、波兰、德国和荷兰。


**影像 1：**取自美亚柏科信息公司网站，检索日期为 2019 年 5 月 1 日，显示“安全走廊”战略规画项目。




**影像 2：**美亚柏科受中国公安部指示，为一带一路国家培训数字搜证。该影像于 2019 年 4 月 29 日检索，共列出 19 个国家。


**影像 3：**该图像于 2019 年 9 月 5 日检索，显示了 29 个国家。美亚柏科删除了图像右上角提到的公安部(参见影像 2)。

## 5. 北京和莫斯科的核心科技圈

以下重点说明“互联度”的强度如何导致深广的扩散，并且形成了核心科技圈。与俄罗斯和中国互联度较低的国家，亦即那些不属于“一带一路”或独联体的国家，就较不可能受到信息控制的广泛扩散，故处于俄罗斯和中国科技圈的外缘。

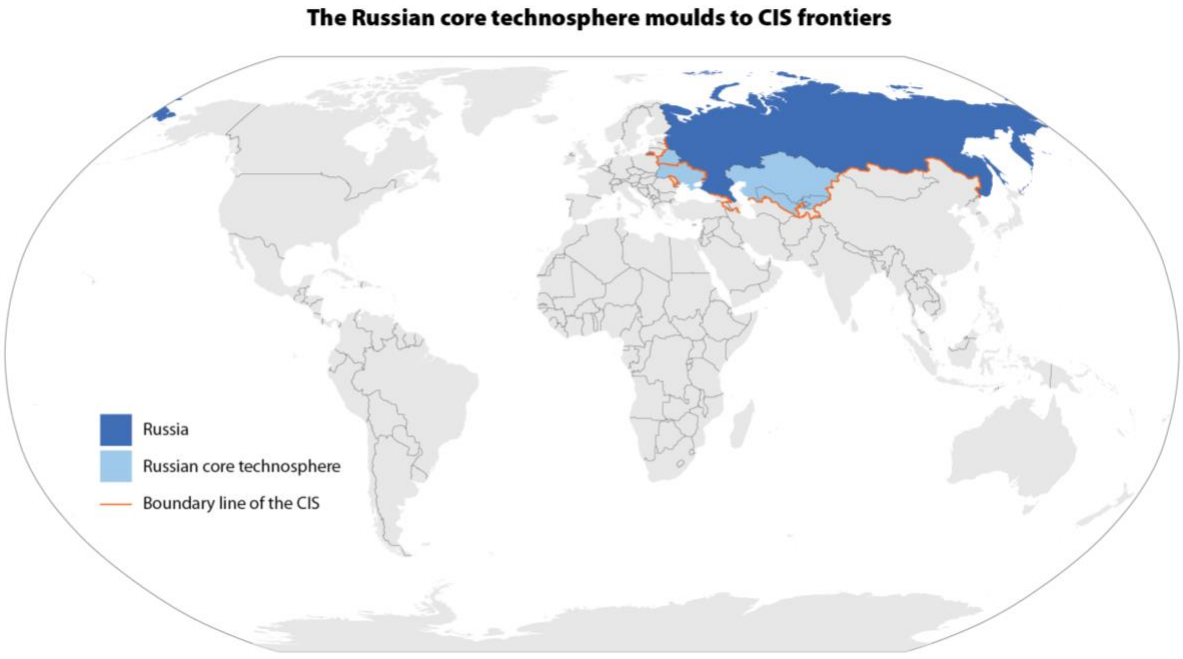
### 独立国家联合体

独联体是 1991 年 12 月苏联解体后成立的，包括亚美尼亚、阿塞拜疆、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、摩尔多瓦、塔吉克斯坦、和乌兹别克斯坦，其目的为鼓励俄罗斯与这些新成立的国家继续在政治、经济、和文化层面合作。乌克兰最初是其中一员，但在 2018 年退出。

本文研究发现，俄罗斯的信息控制扩散到 28 个国家，这些国家的地理位置差很远，如巴勒斯坦和墨西哥天各一方。独联体的国家占俄罗斯信息控制出口的 25%，即在 28 个国家中占 7 国。阿塞拜疆、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、乌克兰、和乌兹别克斯坦位于俄罗斯科技圈的核心。这每一个国家，不论曾经是或现在仍是独联体国家，都已经模仿了俄罗斯的网络监视法律。这些

独联体国家的许多监视法律都带有一种可疑的氛围，制造了威吓异议份子的空间，此即复制了俄罗斯信息控制的做法。然而，如果没有俄罗斯提供的监视技术，仅仅是这些法律与恐惧的环境就没有太大的威力。

白俄罗斯内政部从俄罗斯的一家公司叫 Analytical Business Solutions 购买了技术，这家公司专长在提高网上监看效率。白俄罗斯政府模仿了俄罗斯法律，很可能已经从俄罗斯购买了 SORM 监视设备。哈萨克斯坦从位于圣彼得堡的 VAS Experts 公司购买了深度封包检测技术，取得 iTeco 公司的监看工具，MFI-Soft 公司的 SORM 技术，从 Speech Technology Center 取得 Protei 语音取证工具，以及 Oxygen Software 的移动取证工具。哈萨克紧急事务部也购入 Analytical Business Solutions 提供的信息分析平台 Semantic Archive。吉尔吉斯斯坦从 Oniks-Line 和 Signatek 购买了 SORM 设备。乌克兰还也购入了 SORM 设备。乌兹别克斯坦从 VAS Experts 和 Protei 进口了深度封包检测技术，MFI-Soft 公司的 SORM 设备，Speech Technology Center 的语音取证，以及 Oxygen Software 的移动取证工具。乌兹别克斯坦政府还模仿俄罗斯，制定了国家监视法。




**地图 2：**俄罗斯核心科技圈核心延伸到独联体国家的前线。

**“一带一路”**

“一带一路”倡议于 2013 年正式启动，涵盖 138 个国家；而中国信息控制出口中的 82%是出口到“一带一路”国家(102 国中的 84 国)。该倡议包括连接中国和欧

陆的“丝绸之路经济带”，以及企图恢复以前海路贸易的“21 世纪海上丝绸之路”。跨亚欧大陆的陆线和海上航线还辅以“数字丝绸之路”(Digital Silk Road)，希望以数字科技合作将各国与中国串连一起。

本小节将检视十个参与“一带一路”的国家，显现此处信息控制扩散最为深入(依三个扩散指标)。这些国家成为中国科技圈的核心。

中国在埃及具强大影响力。关于监视科技的移转，华为在该国建立了一个安全城市，海康威视为苏伊士省公交车队提供了闭路电视摄像机。除了这些技术转让外，埃及记者到北京参加由“中国公共外交协会”安排为期十个月的媒体学人计划。他们参访了人民日报的媒体设备，接触到专制媒体天地。埃及官员则参访了美亚柏科，了解数字取证。埃及与中国的合作继续深化。在 2014 年，埃及与中国签署了一项打击网络犯罪的条约。四年后，埃及通过了一项网络犯罪法，规范社交媒体，模仿中国处理社交媒体平台的做法。

伊朗也受到中国使用信息控制的重大影响。最早出口到伊朗的监视设备之一是华为出售的设备，使政府机构可以读取手机。另一家中国公司，中兴通讯，也向伊朗出售监视设备，可用于拦截民众通讯。两国的技术合作在 2014 年更进一步，当时中国和伊朗中央级官员会晤，两国同意由中国协助伊朗布建伊朗国家信息网。伊朗投桃报李，表达一直非常愿意向中国学习。伊朗开发的 Soroush messenger app 全面引用中国国内的应用程序生态系统，允许政府读取。伊朗的信息技术组织(Information Technology Organization)负责人称赞中国“在信息科技应用服务开发方面有四十年的良好经验”，并强调“我们希望能使用这些经验。”

马来西亚是另一个位于中国科技圈核心的国家。马来西亚的记者参访了北京，接受了由中国外交部、教育部、和国有企业华能工业合办的培训项目。一位中国传媒大学的教授指出，这些经历“可以成为受训者在其本国发展媒体产业的蓝图。”培训不只限于记者。总部设在厦门的网络安全公司美亚柏科在马来西亚安排举办了的数位取证培训课程，教导如何从手机和计算器中读取数据。该公司提供培训时指出，“美亚柏科坚守‘迈向全球’的战略和‘一带一路’倡议，一以贯之。”在科技方面，马来西亚一直热衷于买入中国的监视技术。例如，它已经向上海的依图科技公司为治安人员买入全身摄像头。此外，它还从阿里巴巴集团取得了一个人工智能交通管理控制系统，用来监看吉隆坡的交通状况。马来西亚似乎打算延续此一政策方向，首相马哈迪最近宣布，马来西亚将尽可能地多用华为设备。此外，马来西亚前副总理阿迈德扎希哈迈表示，中国缜密使用监视设备来监看每一个行动，值得模仿。

俄罗斯一直热衷于模仿中国更精密的网上内容过滤技术。只过滤特定内容，而非整个网站，可降低超塞的可能性。中国防火墙的工程设计师被邀请到俄罗斯分享技术，以加强合作。中国的培训和技术也扩散到俄罗斯。美亚柏科也对俄罗斯专家提供了数字搜证培训。华为的安全城市解决方案已在圣彼得堡实现；华为提供了“专为大规模视像数据存储和分析而设计”的云存储解决方案。

坦桑尼亚是一个极佳的例子，说明信息控制的扩散是近似线性的方式，一开始是技术转移，然后是培训，最后进展到模仿。在 2014 年，华为宣布，已经在坦桑尼亚布建了一座安全城市。第二年，总部位于杭州的浙江大华技术公司为桑给巴尔总统办公室装配了智能相机，能够辨识面部和声音。一年后，人民日报报导，坦桑尼亚记者参加了由中国公共外交协会主办的媒体学人计划。随后，坦桑尼亚和中国之间更强化的联系促使坦桑尼亚政府努力模仿中国式的审查概念。坦桑尼亚前运输通信部副部长 Edwin Ngonyani，在由坦桑尼亚政府和中国国家互联网信息办公室合办的中坦新媒体圆桌会议上，慨然宣称："我们的中国朋友在他们的国家已经办到了封锁这种媒体，并用他们自建、既安全、有建设性、又受欢迎的网站取而代之。我们还未到那一步，当我们仍在使用这些平台之际，应该防止其中的误用。"

泰国是中国监视科技成功出口的另一个案例。海康威视接下了为泰国商务部提供闭路电视监视的项目，并为泰国警方提供了携带式录象机，能实时录像和远程监看。华为与泰国警方合作，实施 eLTE 集线合作创新项目(eLTE Trunking Joint Innovation Project)监视解决方案。与其他"一带一路"各国情况一样，美亚柏科已经培训了泰国移动和计算器搜证专家，泰国记者也在中国接受了媒体培训。泰国进一步表示，打算从中国依样学样，创建自己的长城防火墙。虽然泰国建立单一网络网关的初步计划已经中止，但是最近有一条法律已经生效，模仿了中国 2017 年通过的模糊又广泛的网络安全法，准许政府对公司和个人财产进行入侵性现场检查。

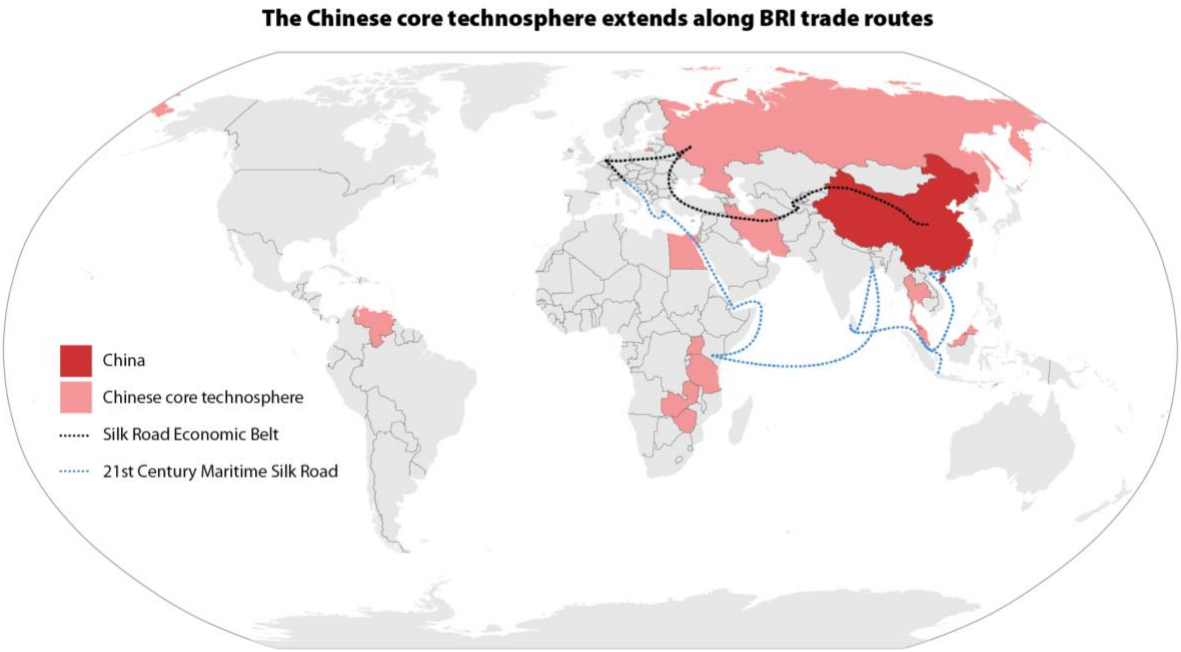
乌干达与中国的信息控制合作范围广泛，稳步推展。在 2017 年，乌干达官员前往北京，会见了国企"中国电子进出口有限公司"(CEIEC)的代表。双方同意，中电将帮助乌干达监看社交媒体和其他"网络犯罪"相关服务。同年，乌干达记者参加了由中国公共外交协会主办，在位于北京的中非新闻中心，进行为期 10 个月的媒体培训。次年，总部位于深圳的华为交付乌干达政府 900 台监视摄像头，支持该国的智能警务计划，还协助政府读取反对派人士的加密通信。最后，在 2019 年 6 月，乌干达通信委员会公布了一项互联网监管草案，规划集中控制进出该国的国际信息流。此一做法非常类似泰国打算建立单一的国际网络网关。据乌干达一位主管法规流程的内部人士指出，"这将把乌干达内的互联网，转变为类似中国集中控制的做法，建置一个中心系统，控制一切。"

赞比亚与中国之间广泛的互联度说明该国位于中国科技圈的核心。为了控制其国民，赞比亚政府依靠华为和中兴通讯提供的审查和监视设备。据称，华为员工协助赞比亚政府拦截记者和反对派团体的数字通讯。华为还实施了一个智能城市，增强赞比亚的实体监控能力。此外，在中国参加了媒体培训的赞比亚记

者对该国的媒体界具有相当的影响力。一位赞比亚部长指出，赞比亚沿着“中国的道路”管理互联网。

赞比亚之南的津巴布韦与中国在信息控制方面有长期合作。早在 2005 年就有报导指出，中国当时正在商谈销售通信拦截设备给津巴布韦，此后疑虑四起，中国的设备用在干扰无线电传播。这些事例是中国出口审查技术的最早例子，之后，中国手段精进。除了阻绝广播内容外，一些中国公司还提供了监视设备。总部位于杭州的海康威视与津巴布韦的“国家硬件和电气”(Nations Hardware and Electrical)公司合作，在该国布建更广泛的闭路电视涵盖面。同样，云从科技公司(Cloudwalk Technology Co.)也提供面部识别摄像头，可能涵盖铁路与机场，以及一个全国性人脸数据库等等。最晚自 2011 年起，津巴布韦记者接受了信息散发技术培训(引导对话、在专制环境中管理媒体)。津巴布韦一直在模仿中国，也直言不讳。该国正在开发等同于社交媒体平台的本土 app，以加强管控。在 2016 年，前津巴布韦信息通信技术部长 Supa Mandiwanzira 说：“总统[穆加贝]说，让我们着手做吧，而且我们正在做。他举中国为例，中国在保护互联网的完整性上，已经发展到相当规模了。”

尽管委内瑞拉的地理位置并非位于「一带一路」的陆线或海线，该国仍是“一带一路”的一部分，也处于中国科技圈的核心。在 2008 年全球金融危机爆发前不久，在当时中国国家主席胡锦涛和委内瑞拉总统查维兹领导下，两国关系开始加温与深化。更紧密的双边合作与互联度也转化成两国在监视方面的合作。在 2008 年，委内瑞拉司法部官员访问深圳，学习国民身份证(national ID card)。在委内瑞拉政府眼中，身份证是个值得效仿的项目。大约十年后，在位于深圳的中兴通讯协助下，委内瑞拉正在实施一种新的智能身分证，也称为“祖国卡”(fatherland card)，或西班牙文 *carnet de la patria* 所称的“国内卡”。该卡包含大量信息，不只是出生年月日、家庭数据，还包括就医纪录、社交媒体活动、党籍、以及是否在选举中投过票。卡片上的信息可鼓励某类行为，如，做个良民。换句话说，中国的社会信用体系靠着「大数据收集和分析，以监看、形塑和评比在经济和社会过程的行为」，不再限于中国。然而，中国和委内瑞拉之间的监视合作还尤有甚之。为了让委内瑞拉官员对人民有更多的控制，华为、中兴、以及中电在委国全境内，建制了多座智能城市和安装数千台闭路电视摄像机。同时，华为也替委内瑞拉技术专家提供系统操作的培训。




**地图 3：**中国沿着“一带一路”贸易路线所建的核心科技圈。

### 重迭的科技圈

中国科技圈和俄罗斯科技圈在总共 20 个国家发生重迭。有趣的是，深处于俄罗斯科技圈的每一个国家，也部分处于中国的科技圈内。中国在白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、乌克兰、和乌兹别克斯坦都很活跃。另一方面，俄罗斯在其邻国以外，只出现在中国科技圈核心诸国中的一国；在泰国，有一家专门进行声音取证的俄罗斯公司 Speech Technology Center 一直在提供设备。

## 6. 扩散的影响

本文讨论扩散的主要结果是创建了“科技圈”，这是一个地理区，却给信息控制出口国取得了各种先占优势。这些优势可分成政治、经济、和情报相关的优势。在政治上，信息控制的增生强化了专制政权。例如，俄罗斯信息安全观的广泛采用，有助于俄国政府对内巩固其合法性，因为政府可以宣传其模式受到国外模仿的此一事实。俄罗斯把信息控制系统扩散海外，俨然奠定其规范制定者的形象。中国对外国政府官员和记者提供培训，与海外领导人物打好关系，让他们了解中国所认知威权信息环境应如何运作。可能会有人质疑，培训某一国中的一些政府官员或记者会有影响吗，但是，在全球层次，培训数以千计的人可能会带来大幅的结构变化，进而使各国只有更依赖中国的设备和技术。美

亚柏科的信息安全学院已经培训了 1000 多名海外执法人员进行数字取证，而中国公共外交协会计划到 2020 年每年培训 1,500 名外国记者。

**影像 4：**百色干部学院，东南亚记者和官员在此接受中国信息控制培训。

在经济上，信息控制的扩散为出口国创造了新的市场。在中国和俄罗斯，已经形成了类似于军工产业体。此一安全工业综合体的组成包括依赖安全相关产业、民间保安公司、和警方的政客。其中的每一实体单位与每个人都得利于国内提高的保安支出和国外出口。信息控制为中国的海康威视、华为，俄罗斯的 Protei 以及 VAS Experts 等监视和审查设备公司创造了营收。信息控制技术的出口对中国来说是一个“双赢”。例如，厄瓜多尔卖石油给中国，回收中国相关监视的采购。如此为中国创造了更多的就业和收入。

将信息控制扩散到科技圈也创造情报使用之虞。例如，中国把非洲联盟(African Union)的总部建在埃赛俄比亚国的亚的斯亚贝巴(Addis Ababa)，据称，已经把安装当地计算器系统中的大量数据传送回中国。中国可能转而利用这些情报，更有效的实现其在非洲大陆的外交政策目标。在巴基斯坦，华为提供的闭路电视摄像机中发现了莫名的 Wi-Fi 模块，有汲取信息风险之虞，换言之，监视产品的出口可能让这个出口国取得了情报好处。值得注意的是，并非仅仅只有中国希望保留能读取已经出口的设备。向吉尔吉斯斯坦提供监视装备的多家俄罗斯公司被指控在系统中留有后门，在系统安装后，让这些公司仍能继续读取讯息。

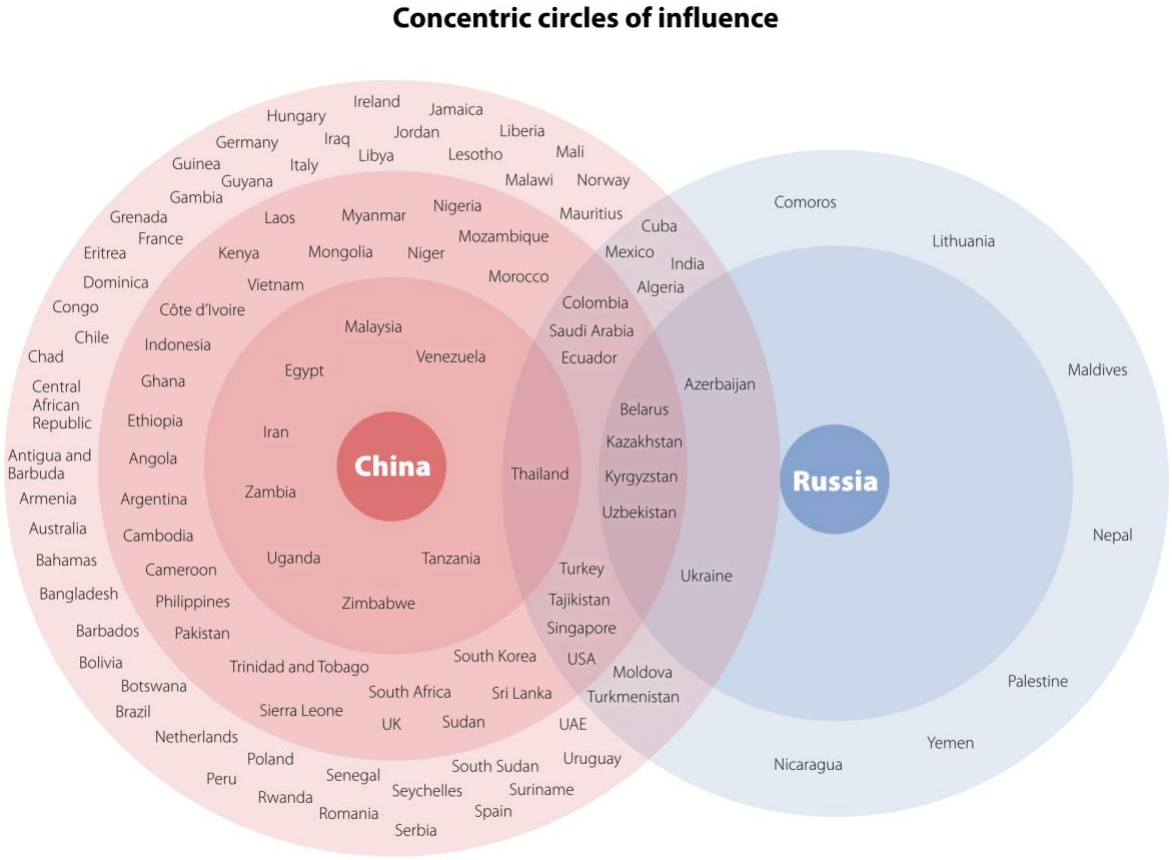
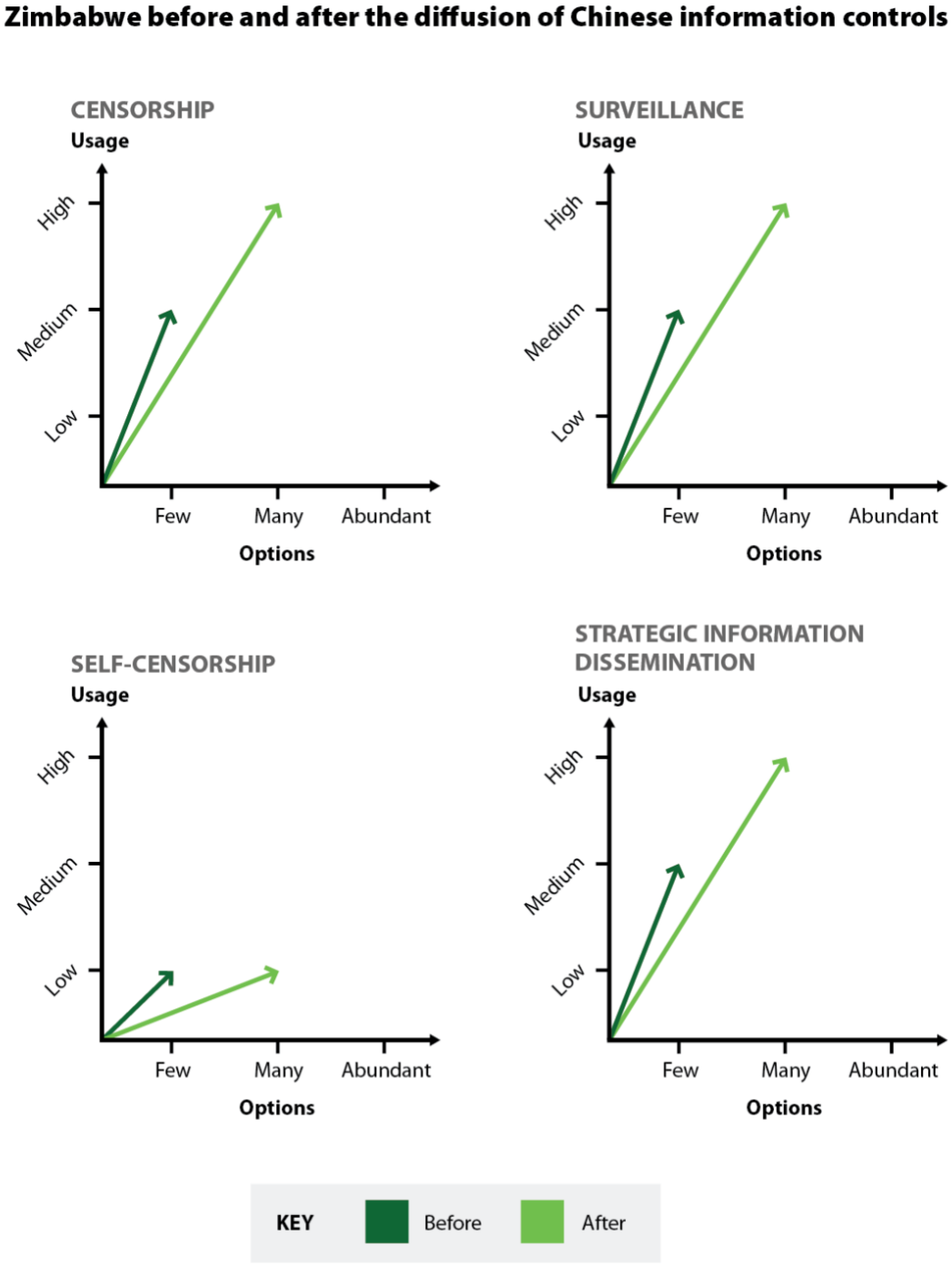



**图 1：**影响力的同心圆。内圈代表核心，往外代表科技圈的外缘。

扩散愈广也会影响信息控制在全球的实施和运用。以津巴布韦为例，本文指出，审查和监视科技以及宣传培训是中国向该国的主要出口。这种扩散确实增加了津巴布韦通过监视科技引起恐惧的选项，以及审查与操纵其民众的能力。换言之，中国对津巴布韦出口提升，使该国有了更多的信息控制选项。同时，信息控制的使用可能随扩散而改变。津巴布韦可能原本只选择仰赖审查和战略信息散发，但与中国的互动肯定使此一非洲国家更能全面采用此一做法。津巴

布韦与中国信息管理方式逐渐融合，在前者明言要模仿后者之时，已经不言可喻。




**津巴布韦的选项：中国信息控制扩散前与扩散后**

**图 5-8：**扩散对津巴布韦的影响。全面深入研究津巴布韦信息控制超出了本文的范围。因此，上述描述中国信息控制在该国扩散之前与之后的四图是假设的。

然而，在扩散过程中，该国向中国模式趋同并非假设，而是基于本文收集的证据。

## 结论

本文综观大约十三年以来中国和俄罗斯的信息控制出口。在此期间，扩散的科技在本质上发生了巨变。最初，大多是粗糙的审查和监视科技往国际扩散。这包括了中国装置，出口到津巴布韦干扰无线电广播，以及俄罗斯提供给前苏联国家的过滤和语音取证设备。逐渐，这些出口展现多样化，早期的初级品变得精良。现在我们正在研究扩散的是具面部识别技术的闭路电视摄像机、形形色色的数字搜证工具、智能国家身份证、政府智能数据库和智能城市。

在这个瞬息万变的环境中，重要的是追踪俄罗斯和中国正在从事何种开发和部署，以便预测国外明天会发生何事。当然，伊朗、泰国、和委内瑞拉等国家都在开发各自的技术和科技，然而，了解俄罗斯和中国信息控制在各国醒目的存在，是辨识它们扩散全球趋势的重要研究起点。

那么，面对这些趋势，民主国家该如何因应？不幸的是，没有简单的答案 -- 部分原因是难以阻止军民两用信息控制科技和技术的散布(更不讳言，民主国家自己也热衷购买信息控制设备)。当培训被描述成善意提供，而非战略信息扩散技术的分享渠道时，即不能受到无的放矢。

尽管如此，民主国家仍然可以采取行动。在国内，民主国家不必部署所有具高度监视功能的工具。麻萨诸塞州正在考虑立法，限制面部识别的使用。旧金山已经通过了此一措施。当民主国家的本国公司参与生产审查和监督技术时，政府应该确保这些公司不会对人权构成滥用或助长滥用。
民主国家还应努力使个人装置和通信渠道更能抵抗过滤或监视设备。然而，现状是正如其反。最近，澳大利亚通过了一项法律，扩张监视，侵害了点对点的加密信息，而这种做法比较在威权政权中常见。加拿大、新西兰、英国、和美国打算让主管当局能够进入存取点。这些做法不必然是维护安全。研究指出，即使不能读取信息，政府当局仍有许多途径可以打击犯罪。点对点加密并不意味着“暗中摸索。”例如，元数据可用来侦防犯罪 -- 而且这通常比私人信息的内容更有用。

最后，无庸置疑，在民主国家，公权力使用监视装置时，应遵循透明、由公众问责的程序。例如，应订定制衡机制，使只能让当地警察接触的监视设备，不被国家情报机构取得。

虽然这些建议本身都不能阻止监控技术在全球散布，但是全面的防范可以降低未来可能的滥用。

全球言论表达自由和人权状况逐渐恶化。迄今为止，超过一百多个国家已经购入与模仿俄罗斯和中国的信息控制，并且接受过这两国的培训。有鉴于此一趋势，民主国家需要众志成城，反对技术为威权所用，并向世界展示，各国政府可以既打击犯罪又确保国家安全，同时不会弱化网络安全 – 以及民众的隐私。这当然并非易事，但是值得努力。如果民主国家不采取行动，还有谁呢？

## 感谢

我非常感谢 Lucas Kello 和 Joss Wright，在本文写作的各个阶段提供的洞见、建议和指导。我从 Irene Poetranto、Gabrielle Lim、Max Kuhelj-Bugaric、Jonas Kaiser 和 Dean Jackson 的评论中获益匪浅。我也非常感谢哈佛大学“伯克曼克莱因互联网与社会中心”(Berkman Klein Center for Internet and Society)提供我思考的空间，以及“开放技术基金会”(Open Technology Fund)与“英国工程与物理科学研究委员会”(UK Engineering and Physical Science Research Council)慷慨支持我的研究。

## 附录 A:扩散表

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 阿尔及利亚 C(1) R(1) | A | X | X | | | | |
| 安哥拉 C(2) | A | X | | | | X | |
| 安提瓜及巴布达 C(1) | / | | | | | X | |
| 阿根廷 C(2) | D | X | | | | X | |
| 亚美尼亚 C(1) | H | | | | | X | |
| 澳大利亚 C(1) | D | | | | | X | |
| 阿塞拜疆 C(1) R(2) | A | X | X | | X | | |
| 巴哈马 C(1) | / | | | | | X | |
| 孟加拉国国 C(1) | H | | | | | X | |
| 巴巴多斯 C(1) | / | | | | | X | |
| 白俄罗斯 C(2) R(2) | A | X | X | | X | X | |
| 玻利维亚 C(1) | H | X | | | | | |
| 博茨瓦纳 C(1) | D | | | | | X | |
| 巴西 C(1) | D | X | | | | | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 柬埔寨 C(2) | A | X | | | | X | |
| 喀麦隆 C(2) | A | X | | | | X | |
| 乍得 C(1) | A | | | | | X | |
| 中非共和国 C(1) | A | | | | | X | |
| 智利 C(1) | D | X | | | | | |
| 中国 R(1) | A | N/A | | N/A | X | N/A | |
| 哥伦比亚 C(2) R(1) | D | X | X | | | X | |
| 科摩罗 R(1) | A | | X | | | | |
| 刚果 C(1) | A | | | | | X | |
| 科特迪瓦 C(2) | H | X | | | | X | |
| 古巴 C(1) R(1) | A | X | X | | | | |
| 多米尼克 C(1) | / | | | | | X | |
| 厄瓜多尔 C(2) R(1) | D | X | X | | | X | |
| 埃及 C(3) | A | X | | X | | X | |
| 厄立特里亚 C(1) | A | | | | | X | |
| 埃赛俄比亚 C(2) | A | X | | | | X | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 法国 C(1) | D | X | | | | | |
| 冈比亚 C(1) | H | | | | | X | |
| 德国 C(1) | D | X | | | | | |
| 加纳 C(2) | D | X | | | | X | |
| 格林纳达 C(1) | / | | | | | X | |
| 几内亚 C(1) | A | | | | | X | |
| 圭亚那 C(1) | D | | | | | X | |
| 匈牙利 C(1) | D | X | | | | | |
| 印度 C(1) R(1) | D | | X | | | X | |
| 印度尼西亚 C(2) | D | X | | | | X | |
| 伊朗 C(3) | A | X | | X | | X | |
| 伊拉克 C(1) | H | X | | | | | |
| 爱尔兰 C(1) | D | X | | | | | |
| 约旦 C(1) | A | X | | | | | |
| 意大利 C(1) | D | X | | | | | |
| 牙买加 C(1) | D | | | | | X | |
| 哈萨克斯坦 C(2) R(2) | A | X | X | | X | X | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 肯尼亚 C(2) | H | X | | | | X | |
| 吉尔吉斯斯坦 C(2) R(2) | H | X | X | | X | X | |
| 老挝 C(2) | A | X | | | | X | |
| 莱索托 C(1) | D | | | | | X | |
| 利比里亚 C(1) | H | | | | | X | |
| 利比亚 C(1) | A | X | | | | | |
| 立陶宛 R(1) | D | | X | | | | |
| 马拉威 C(1) | H | | | | | X | |
| 马来西亚 C(3) | D | X | | X | | X | |
| 马尔代夫 R(1) | / | | X | | | | |
| 马里 C(1) | H | | | | | X | |
| 毛里求斯 C(1) | D | X | | | | | |
| 墨西哥 C(1) R(1) | D | X | X | | | | |
| 摩尔多瓦 C(1) R(1) | H | X | | | X | | |
| 蒙古 C(2) | D | X | | | | X | |
| 摩洛哥 C(2) | H | X | | | | X | |
| 莫桑比克 C(2) | A | X | | | | X | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 缅甸 C(2) | A | X | | | | X | |
| 尼泊尔 R(1) | H | | X | | | | |
| 荷兰 C(1) | D | X | | | | | |
| 尼加拉瓜 R(1) | A | | X | | | | |
| 尼日尔 C(2) | A | X | | | | X | |
| 尼日利亚 C(2) | H | X | | | | X | |
| 挪威 C(1) | D | X | | | | | |
| 巴基斯坦 C(2) | H | X | | | | X | |
| 巴勒斯坦 R(1) | H | | X | | | | |
| 秘鲁 C(1) | D | | | | | X | |
| 菲律宾 C(2) | D | X | | | | X | |
| 波兰 C(1) | D | X | | | | | |
| 罗马尼亚 C(1) | D | X | | | | | |
| 俄罗斯 C(3) | A | X | N/A | X | N/A | X | N/A |
| 卢旺达 C(1) | A | | | | | X | |
| 沙特阿拉伯 C(2) R(1) | A | X | X | | | X | |
| 塞内加尔 C(1) | D | X | | | | | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 塞尔维亚 C(1) | D | X | | | | | |
| 塞舌尔 C(1) | / | | | | | X | |
| 赛拉利昂 C(2) | H | X | | | | X | |
| 新加坡 C(2) R(1) | D | X | X | | | X | |
| 南非 C(2) | D | X | | | | X | |
| 韩国 C(2) | D | X | | | | X | |
| 南苏丹 C(1) | / | | | | | X | |
| 西班牙 C(1) | D | X | | | | | |
| 斯里兰卡 C(2) | D | X | | | | X | |
| 苏丹 C(2) | A | X | | | | X | |
| 苏里南 C(1) | D | | | | | X | |
| 塔吉克斯坦 C(2) R(1) | A | X | X | | | X | |
| 坦桑尼亚 C(3) | H | X | | X | | X | |
| 泰国 C(3) R(1) | H | X | X | X | | X | |
| 特立尼达与多巴哥 C(2) | D | X | | | | X | |
| 土耳其 C(2), R(1) | H | X | X | | | X | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 土库曼斯坦 C(1), R(1) | A | | X | | | X | |
| 乌干达 C(3) | H | X | | X | | X | |
| 乌克兰 C(1), R(2) | H | X | X | | X | | |
| 阿拉伯联合酋长国 C(1) | A | X | | | | | |
| 英国 C(2) | D | X | | | | X | |
| 美国 C(2), R(1) | D | X | X | | | X | |
| 乌拉圭 C(1) | D | X | | | | | |
| 乌兹别克斯坦 C(2) R(2) | A | X | X | | X | X | |
| 委内瑞拉 C(3) | A | X | | X | | X | |
| 越南 C(2) | A | | | X | | X | |
| 也门 R(1) | A | | X | | | | |
| 赞比亚 C(3) | H | X | | X | | X | |
| 津巴布韦 C(3) | A | X | | X | | X | |
| 计(共 110) | | 73 | 26 | 11 | 8 | 75 | 0 |
| 俄罗斯式扩散 | | 俄罗斯信息控制扩散至 28 国。 | | | | | |

| | 政体类 | 过滤或监视科技 | | 模仿 | | 培训 | |
|---|---|---|---|---|---|---|---|
| 国家 | | **中国** | **俄罗斯** | **中国** | **俄罗斯** | **中国** | **俄罗斯** |
| 中国式扩散 | | 中国信息控制扩散至 102 国。 | | | | | |
| 合并扩散 | | 俄罗斯和中国的信息控制扩散到 110 个国家(含两国模式相互扩散）。信息控制出口到 41 个民主体制，24 个混合制政体，37 个威权式政权，本文研究共 8 个国家没有在经济学人的政权类型数据库列出其政权类型：安堤瓜及巴布达、巴哈马、巴巴多斯、多米尼克、格林纳达、马尔代夫、塞舌尔和南苏丹。 | | | | | |

## 附录 B：中国公司表

| 公司 | 科技类别/参与 | 总部位于 | 扩散到 |
|---|---|---|---|
| Alcatel-Lucent 上海贝尔公司 | SORM 兼容设备 | 上海 | 哈萨克斯坦 |
| 阿里巴巴集团 | 人工智能流量管理控制系统 | 杭州 | 马来西亚 |
| 百分点公司 | AI 大数据库管理系统 | 北京 | 安哥拉 |
| 中国电子进出口有限公司 | 安全城市 | 北京 | 厄瓜多尔、特立尼达和多巴哥、乌干达、委内瑞拉 |
| 云从科技 | 面部辨识摄像机 | 北京 | 津巴布韦 |
| 浙江大华技术公司 | 面部辨识摄像机 | 杭州 | 坦桑尼亚 |
| 海康威视 | 面部辨识摄像机 | 杭州 | 阿根廷、巴西、埃及、爱尔兰、约旦、缅甸、南非、韩国、泰国、乌克兰、英国、津巴布韦 |
| 华能集团 | 支持媒体培训 | 北京 | 孟加拉国、马来西亚 |

| 公司 | 科技类别/参与 | 总部位于 | 扩散到 |
| --- | --- | --- | --- |
| 华为 | 审查技术、面部辨识摄像机、安全城市、协助政府读取加密通讯 | 深圳 | 阿尔及利亚、阿塞拜疆、白俄罗斯、玻利维亚、喀麦隆、智利、哥伦比亚、科特迪瓦、古巴、厄瓜多尔、埃及、法国、德国、加纳、匈牙利、印度尼西亚、伊朗、伊拉克、意大利、肯尼亚、老挝、墨西哥、摩尔多瓦、摩洛哥、莫桑比克、尼日尔、尼日利亚、荷兰、挪威、巴基斯坦、菲律宾、波兰、俄罗斯、沙特阿拉伯、塞尔维亚、新加坡、西班牙、塔吉克斯坦、坦桑尼亚、泰国、特立尼达和多巴哥、土耳其、乌干达、乌克兰，阿拉伯联合酋长国、美国、委内瑞拉、赞比亚 |

| 公司 | 科技类别/参与 | 总部位于 | 扩散到 |
| --- | --- | --- | --- |
| 美亚柏科 | 数字取证与网络安全培训 | 厦门 | 阿根廷、亚美尼亚、孟加拉国国、白俄罗斯、柬埔寨、哥伦比亚、厄瓜多尔、埃及、印度、印度尼西亚、哈萨克斯坦、吉尔吉斯斯坦、老挝、马来西亚、蒙古、摩洛哥、缅甸、巴基斯坦、菲律宾、俄罗斯、沙特阿拉伯、新加坡、南非、泰国、塔吉克斯坦，土库曼斯坦、土耳其、乌兹别克斯坦、英国、越南 |
| 商汤科技 | 动态面部识别人控制系统 | 北京 | 蒙古 |
| 依图科技 | 面部辨识摄像机 | 上海 | 马来西亚 |
| 中兴通讯 | 审查科技、安全城市 | 深圳 | 白俄罗斯、埃塞俄比亚、利比亚、罗马尼亚、塞内加尔、塞拉利昂、斯里兰卡、苏丹、乌拉圭、委内瑞拉、赞比亚 |

## 附录 C：与中国有关的实体单位

| 实体单位 | 角色 | 总部位于 | 扩散到 |
| --- | --- | --- | --- |
| 澳大利亚-中国关系研究院 | 主办记者中国学习参访团 | 悉尼、澳大利亚 | 澳大利亚 |
| 中国菲律宾大使馆 | 提供记者与官员媒体培训 | 北京 | 菲律宾 |
| 中国外交出版发行事业局 | 提供记者与官员媒体培训 | 北京 | 菲律宾 |
| 中国公共外交协会 | 协调媒体培训 | 北京 | 安哥拉、安堤瓜及巴布达、巴哈马、巴巴多斯、博茨瓦纳、喀麦隆、乍得、中非共和国、刚果、科特迪瓦、多米尼克、埃及、厄立特里亚、冈比亚、加纳、格林纳达、几内亚、圭亚那、牙买加、肯尼亚、莱索托、利比里亚、马拉维、马里、莫桑比克、尼日尔、尼日利亚、巴基斯坦、卢旺达、塞舌尔、塞拉利昂、南非、南苏丹、苏丹、苏里南、乌干达 |
| 中美交流基金会 | 组织记者访问华团 | 香港 | 美国 |
| 中国传媒大学 | 举行媒体培训 s | 北京 | 孟加拉国国、马来西亚 |
| 国务院新闻办公室 | 与官员与记者分享信息控制技术 | 北京 | 伊朗、菲律宾 |

| 实体单位 | 角色 | 总部位于 | 扩散到 |
|---|---|---|---|
| 广西共产党人事单位 | 办理百色干部学院 | 广西地区 | 老挝、缅甸、越南 |
| 商务部 | 记者与官员媒体培训 | 北京 | 菲律宾 |
| 教育部 | 支持媒体培训 | 北京 | 孟加拉国国、马来西亚 |
| 外交部 | 支持媒体培训 | 北京 | 孟加拉国国、马来西亚 |
| 公安部 | 与柬埔寨执法单位的监视设备合作 | 北京 | 柬埔寨 |
| 人民解放军情报部 | 训练官员进行信息控制 | 北京 | 斯里兰卡 |
| 清华大学 | 全球商务记者计划 | 北京 | 韩国 |

## 附录 D: 俄罗斯公司表

| 公司 | 科技类别/参与 | 总部位于 | 扩散到 |
|---|---|---|---|
| Analytical Business Solutions | 用于分析论坛和社交媒体平台中的开放来源数据工具 | 莫斯科 | 白俄罗斯、哈萨克斯坦 |
| iTeco | 用于分析论坛和社交媒体平台中的开放来源数据工具 | 莫斯科 | 哈萨克斯坦 |
| MFI - Soft | SORM 设备 | 下诺夫哥罗德与莫斯科 | 哈萨克斯坦、塔吉克斯坦、乌兹别克斯坦 |
| Oniks – Line | SORM 设备 | 莫斯科 | 吉尔吉斯斯坦 |

| 公司 | 科技类别/参与 | 总部位于 | 扩散到 |
| --- | --- | --- | --- |
| Oxygen Software | 移动搜证 | 莫斯科 | 哈萨克斯坦、乌兹别克斯坦 |
| Protei | SORM 设备 | 圣彼得堡 | 科摩罗、古巴、哈萨克斯坦、巴勒斯坦、塔吉克斯坦、乌兹别克斯坦 |
| Signatek | SORM 设备 | 新西伯利亚 | 吉尔吉斯斯坦 |
| Speech Technology Center (STC) / SpeechPro | 语音取证/面部辨识 | 圣彼得堡 | 阿尔及利亚、哥伦比亚、厄瓜多尔、印度、哈萨克斯坦、马尔代夫、墨西哥、尼泊尔、沙特阿拉伯、新加坡、土库曼斯坦、土耳其、美国、乌兹别克斯坦、也门 |
| VAS Experts | SORM 设备 | 圣彼得堡 | 阿塞拜疆，哈萨克斯坦，立陶宛，尼加拉瓜，乌兹别克斯坦 |