http://fddi.fudan.edu.cn

复旦智库

THINK TANKS FUDAN

复 旦 智 库 报 告

FUDAN REPORT SERIES

2020 NO.6(29)

未来系列

PIONEER INSIGHT

清洁网络计划与美国数字霸权

复旦发展研究院
复旦大学网络空间国际治理研究基地
复旦大学中国网络空间战略研究所

清洁网络计划与美国数字霸权

沈逸 江天骄 主编

复旦发展研究院

复旦大学网络空间国际治理研究基地

复旦大学中国网络空间战略研究所

2020 年 9 月 7 日

课题团队成员

课题组组长：沈逸　复旦发展研究院教授

复旦大学网络空间国际治理研究基地主任

课题组副组长：江天骄 复旦发展研究院讲师

复旦大学网络空间国际治理研究基地主任助理

课题组成员：雷婷 复旦大学中国网络空间战略研究所科研助理

陆滨 复旦大学中国网络空间战略研究所科研助理

朱嘉豪 复旦大学中国网络空间战略研究所科研助理

高瑜 复旦大学国际关系与公共事务学院博士研究生

宫云牧 复旦大学国际关系与公共事务学院博士研究生

目录

摘要

2020 年 6 月,美国提出清洁网络（Clean Network）计划，包括通过制订清洁网络名单,采取综合措施保护美国公民的隐私和公司敏感信息免受所谓中国等恶意行为者的侵扰。该计划于 8 月 5 日更新，在 5G 清洁路径计划的基础上推出了五项新的计划来保护美国的关键电信和技术基础设施。清洁网络计划基本覆盖全供应链生态闭环，是美国在对中国网络产业长期研究和深度解剖基础上提出的精准打击策略，可以看作是实现其数字霸权的一套工具箱。

清洁网络计划是一个挑战全球信息产业内生规律的非理性构想，其表现形式，是美国政府部门基于高度意识形态化的主观战略认知，以及来源复杂且难以精准表述的混合型需求所制定的模糊的战略构想，其本质是指向全球信息产业供应链安全与稳定的非关税壁垒，目的在于实现具有强可复制性的基于国别和身份的歧视性市场准入控制。清洁网络计划与 5G 清洁路径(5G Clean Path)计划等其他计划一起，构成美国维护和巩固其数字霸权（即地缘政治与金融领域霸权在数字时代的延伸与拓展）的关键举措。

清洁网络计划是美国数字霸权战略的最新产物,目的在于以破坏相关领域行业基本游戏规则的方式,非对称地获取信息领域的主导权。采取这种做法的目的是混合型的，包括：在短期内实现某种非健康态的跃升——让一个事实上不掌握 5G 领域产业优势的国家，以重新定制歧视性和排他性战略，在全球范围内重新获得 5G 领域的主导；在

中长期实体层面不具备产业意义上的压倒性优势的情况下，依托产业和技术之外的手段，防止中国互联网产业对美国主导的全球数字产业形成超越，从而维护美国的数字霸权。

美国的实践，包括制订清洁网络计划等在内，就是通过一系列非技术性的歧视性安排，以诉诸地缘政治与政治猜忌的方式，将正常的商业、行业竞争对手描述为国家威胁，继而采取不尊重市场游戏规则的方式，包括但不限于对客观标准进行主观的随意解释、在实践当中突破常规和默契等，形成显著以美国为中心的扭曲的市场秩序，进而实现对相关行业厂商而言，具有某种非对称掠夺特性的扭曲的市场秩序。这种行为，威胁并挑战了全球范围的商业规则，具有典型的双重标准、单边主义和自我中心等霸权主义特征。

需要指出的是，自 20 世纪 80 年代以来，由于经济发展和技术进步的客观规律，总会有包括美国盟友在内的其他国家及其代表性的跨国企业在国际市场上与美国竞争，甚至威胁到美国的主导地位。对于这些竞争者，美国均通过金融、技术和法律等手段进行严厉的打压。因此，中国绝不是美国数字霸权的唯一受害者，美国的数字霸权对整个国际社会和数字产业都会带来危害。

美国在网络空间构建的是一种支配型的秩序，这种支配型的秩序要保证美国处于压倒性的优势位置，进而追求实现以下四个方面的目标：

第一，客观上美国要处于绝对安全的状态，同时具备压倒性的实力优势，能够对除美国以外的其他行为体，包括国家与非国家，随时

构成致命的威胁；

第二，美国要求在网络空间，以美国及其核心盟友为核心的群体，具备非对称的行动自由，即可以在事实上不受约束地采取任何行为，同时不允许任何其他行为体获得这种自由；

第三，要求美国企业和产业在全产业处于压倒性的领先位置，不允许任何非美企业，包括来自美国盟友的非美企业，在未经美国许可的情况下，形成对美国企业的挑战、威胁或者超越；

第四，美国必须具备根据自身的需求，包括意识形态理念，任意调整全球范围相关产业分工态势的能力，并实现对全球范围各类行为体提升技术能力的实质性有效控制。

整体而言，5G 清洁路径计划是美国数字霸权的初步体现，而清洁网络计划则显示美国为维护其数字霸权已经变得歇斯底里，其可能造成的中长期负面影响与严重损害，已经清晰可见。

对全球所有行为体来说，除非能够保证“永远”不构成与美国政府或者企业的竞争关系，否则始终都面临来自美国网络霸权打压的常态化风险。美国的此类霸权行径，违背产业发展客观规律，将损害其他国家的数字主权，阻碍行业发展。为了应对美国网络空间霸权主义行径给 5G 等新兴技术应用和人类社会发展带来的挑战，让技术真正造福人类，国际社会需要共同努力，保持开放的市场以促进创新和竞争，以客观的标准，和明确告知风险且高度透明的要求作为依据建立采购惯例与准则，建立全球 ICT 供应链安全规范并采取有效措施建立信任，化解清洁网络计划带来的风险。

清洁网络计划与美国数字霸权

前言

2020 年 6 月,美国提出清洁网络计划，包括通过制订清洁网络名单,采取综合措施保护美国公民的隐私和公司敏感信息免受所谓中国等恶意行为者的侵扰。该计划于 8 月 5 日更新，在 5G 清洁路径计划的基础上推出了五项新的计划来保护美国的关键电信和技术基础设施。清洁网络的五项新工作包括：清洁运营商，确保所谓不受信任的中国运营商不与美国电信网络连接；清洁商店，从美国移动应用商店中删除不受信任的应用；清洁应用程序，防止所谓不受信任的中国智能手机制造商在其应用商店中预装（或以其他方式使之可供下载）受信任的应用程序；清洁云，防止美国公民敏感个人信息和企业知识产权在百度、阿里巴巴、腾讯等可被外国对手访问的基于云的系统上进行存储和处理；清洁电缆，确保连接美国与全球互联网的海底电缆不被所谓中国大规模破坏并进行情报收集。

美国的清洁网络计划是基于国家主观战略和需求的行业基础战略，这种判定不是对技术本身进行客观判定，而是以技术来源方的身份属性作为主要判定标准。这种带有主观色彩的意识形态偏见的做法违背产业规律，将会严重扰乱全球产业链。从本质上来说，清洁网络计划是美国维护其数字霸权的关键举措,是在信息产业以供应链安全为由设置的非关税壁垒，其最终目标是维护美国的数字霸权。

需要指出的是,清洁网络计划是美国在对中国网络产业长期研究

和深度解剖基础上提出的精准打击策略，是在中国互联网产业对美国数字霸权形成挑战的背景下，所采取的一种非常态化的手段，其核心特征，就是尝试颠覆性地重构规则，迫使各方以意识形态等非技术因素进行重新站队，继而扭曲和干扰全球市场的正常秩序。

华为、中兴等中国企业不是第一批受害者，在此之前，日本的东芝、法国的阿尔斯通、空中客车等，无论其所在母国与美国的关系如何，均因自身在相关行业取得的成功，而遭遇来自美国的霸凌和打压。

整体来看，自 20 世纪 80 年代以来，由于经济发展和技术进步的客观规律，总会有包括美国盟友在内的其他国家及其代表性的跨国企业在国际市场上与美国竞争，甚至威胁到美国的主导地位。对于这些竞争者，美国均通过金融、技术和法律等手段进行严厉的打压。因此，中国绝不是美国数字霸权的唯一受害者，美国的数字霸权对整个国际社会和数字产业都会带来危害。

美国此次制订清洁网络计划对包括华为在内的中国企业的打压是美国霸权行径的自然延续。在中美战略竞争加剧的今天，中国成为了美国的针对对象。在未来，如果其他国家与美国存在类似的战略竞争，美国很有可能对其他国家采取同样的措施；**甚至在某种极端情况下，如果此类行为模式未能得到有效的矫正继而获得了某种事实上常态化的认可，即使没有形成战略竞争的局面，只要美国不满意自身在相关产业所获得的收益，就可以用类似的方式，通过施压来获取额外的收益。**

一、美国的经济霸权与数字霸权

美国作为世界头号互联网大国，在网络空间一直致力于谋求一种霸权。根据美国的设想，实现其数字霸权最理想的方式是联合盟友在底层掌握对于网络的控制权，进而通过美国的高科技企业以提供互联网服务的方式在各国渗透，在云端进行数据控制，最后通过掌握的数据与情报网络一起组成协同平台，实现其数字霸权并服务于自身国家利益。美国的数字霸权建立在美国的经济霸权基础之上，两次世界大战帮助美国实现其经济霸权，并一直保持到现在。

1.美国通过两次世界大战建立其经济霸权

第一次世界大战期间，作为非参战国，美国通过售卖军火迅速积累了大量财富。战争时期，政府暂停反托拉斯的行动、推动科学研究进步，以及鼓励军售等举措间接地为战后新兴技术产业的脱颖而出奠定了基础。第一次世界大战结束时，美国已从曾经的负债累累一跃而成为各国的债主，从资本输入国变为资本输出国，从债务国变成了债权国。1920 年，美国开始步入工业化中期阶段，这也是美国正式取代英国，成为世界新霸主的重大转折时期。1939 至 1945 年爆发的第二次世界大战，又为美国带来了一次经济增长的良机，这次战争对于美国财富增长的影响程度之深、影响范围之广都是史无前例的。二战结束时，美国的 GDP 已是英国的 10 倍，其黄金储备为 200 亿美元，几乎占当时世界总量(约 330 亿美元)的三分之二。[1]

也正是在这个时期，美国根据“租借法案”向盟国提供了价值 500

[1] 鲍盛钢：《美国是如何和平崛起的》，《联合早报》，2010 年 5 月 24 日。

多亿美元的货物和劳务。黄金源源不断流入美国，美国的黄金储备从1938 年的 145.1 亿美元增加到 1945 年的 200.8 亿美元，约占世界黄金储备的 59%。美元的国际地位因其国际黄金储备的巨大实力而空前稳固。这使得美国可以建立一个以美元为支柱的有利于美国对外经济扩张的国际货币体系。

1945 年 12 月 27 日，在参加布雷顿森林会议的所有国家中，二十几国代表在《布雷顿森林协定》上签字，正式成立国际货币基金组织和世界银行。从此，开始了国际货币体系发展史上的一个新时期。布雷顿森林体系以黄金为基础，以美元作为最主要的国际储备货币。美元直接与黄金挂钩，各国货币则与美元挂钩，并可按 35 美元一盎司的官价向美国兑换黄金。它使美元在战后国际货币体系中处于中心地位，从此，美元成为了国际清算的支付手段和各国的主要储备货币。

二战临近结束之时，美国就开始在各个领域建立国际机制，填补英国霸权崩溃造成的真空，建构自己的霸权体系。在经济领域，美国主导建立了国际货币基金组织(IMF)、世界银行(WB)、关贸总协定(GATT，即后来的世界贸易组织 WTO)等赖以控制和管理世界经济的国际机制，打造自由主义国际经济秩序。

1945 至 1969 年，美国在这一时期登上了资本主义世界的高峰。以原子能技术、宇航技术、电子计算机技术发展为标志的新科学技术革命在美国兴起，推动美国经济高度现代化发展。此外，美国现代企业组织、国家和国际垄断组织均实现了新的发展，同时跨国公司也迅速崛起。得益于上述条件，美国成为高度现代化的超级大国，并开始

向后工业社会和信息社会转化。以核能、计算机以及空间技术为代表的第三次工业革命推动着全球供应链的转移，使美国成为全球供应链的核心。

2.美国数字霸权的建立以经济霸权为基础

美国的经济霸权助推了其数字霸权的建立。从互联网的发展历史看，美国具有得天独厚的优势，它既是互联网技术最主要的发源地，也是网络根域名解析服务器最大的控制国。美国通过控制网络来控制世界，进而巩固其霸权地位。在第二次世界大战后的第三次科技革命中，美国在资源配置、技术标准、内容生成等方面都处于垄断地位，其对于网络资源分配以及产业链关键环节的主导权，构成了美国数字霸权的基础。[2]目前，包括操作系统、芯片设计、软件等在内，全球互联网产业链上的每个关键环节基本都被美国所主宰。凭借其在网络产业链关键环节的主导权，美国在网络空间拥有了绝对的优势，进而使美国可以在全球开展不受节制的大范围窃听和监听，以实现自身的数字霸权。此外，美国还通过制定全球通用的互联网技术标准，掌握通信领域的控制权。最后，美国通过制定网络空间国际规则，使美国的霸权政策合法化。从奥巴马政府到特朗普政府，美国不断提高网络在国家安全中的地位，出台一系列网络空间战略，巩固其网络空间主导地位，维护其网络霸权。清洁网络计划与美国一系列网络空间国家战略一脉相承，是当前新时期美国为维护其全球数字霸权而利用国家力量强制进行的努力，是美国网络霸权战略在数字行业领域的体现。

[2] 杜雁芸：《美国网络霸权实现的路径分析》，《太平洋学报》2016 年第 2 期，第 66 页。

冷战结束之后，美国一方面凭借其超强的军事能力巩固其在政治和安全领域的霸权；另一方面，随着全球化的深入开展，美国主要依靠金融、技术和法律制度护持其在经济领域的霸权地位。

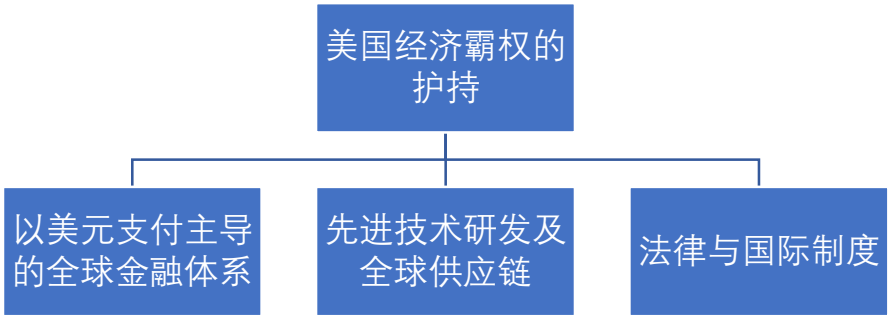

图 1：美国经济霸权体系

二、美国习惯于通过打压竞争性企业维护其经济霸权

由于经济发展和技术进步的客观规律，总会有包括美国的盟友在内（20 世纪 80-90 年代的日本、西欧大国）的其他国家及其代表性的跨国企业在国际市场上与美国竞争，甚至威胁到美国的主导地位。

对于这些竞争者，美国会通过金融、技术和法律三种手段进行严厉的打压。金融方面主要是利用美元霸权的优势地位，实施独特的金融制裁，将相关企业列入制裁名单，迫使其无法使用美元进行交易结算；技术方面包括出口管制禁令，以及通过切割或重组供应链，掐断企业生命线；法律方面，美国起初依赖以 WTO 为代表的国际多边制度，但随着其他国家实力不断增强，对 WTO 法律和程序有了更深入的了解，美国开始认为国际制度效率低下，但本质问题是伴随其他国家的崛起，美国逐渐失去了对国际多边主义平台事实上的有效控制，因此

美国开始退回双边和单边的框架，频繁使用包括 301 调查在内的国内法律程序，借助长臂管辖和实体清单等各种政策工具的不同组合，使“合规问题武器化”，“贸易和技术问题政治化”，并最终发展出了习惯性的“安全化”处置方式，即将上述问题全部人为建构成所谓国家安全问题，继而采取更具主观性和随意性的方式，来护持美国的霸权地位。

1.利用美元支付体系为核心表征的金融霸权工具对相关企业进行制裁和打压

单边金融制裁是美国最强有力的武器之一。这种制裁之所以具有直接的强制性，主要是凭借美元在全球商品、资本交易中的核心地位，其具体实现路径是通过以环球银行金融电信协会（SWIFT）为主的美元跨境资金清算系统与跨境金融基础设施来进行。SWIFT 成立于 1937 年，目前已经为全球 200 多个国家和地区的 11000 多家机构提供安全讯息服务和接口软件。作为以美元主导的国际清算体系的重要组成部分，任何在全球广泛开展业务往来的个人、企业组织和国家等都无法避开 SWIFT，而且美国还可以利用 SWIFT 组成的金融交易网络，通过相关金融数据精确识别制裁目标并制定制裁手段，实行动态监管以保证制裁效果。美国利用美元支付体系对相关企业进行制裁和打压通常出现在美国经济利益受损或市场地位受到威胁时，以美国对“北溪 2 号”项目的制裁为典型。

“北溪 2 号”是俄罗斯与欧盟的天然气合作项目，目标是通过波罗的海和德国，每年向欧盟国家提供 550 亿立方米的天然气。然而，

该项目却受到美国的阻挠。2019 年 1 月，美国驻德国大使格雷内尔警告德国企业，并指出:“‘北溪 2 号’将使乌克兰的安全和政治地位下降，导致俄罗斯介入干预乌克兰冲突的风险上升。此外，欧盟也会因此产生对俄罗斯能源安全的依赖性。所有参与相关项目的企业必须要明白与之相关的企业声誉损失和可能受到的制裁。”

为了打消乌克兰的顾虑，俄罗斯、欧盟和乌克兰三方在欧盟总部布鲁塞尔举行了天然气问题谈判,并于 2019 年 12 月 19 日达成一致。然而，就在次日，美国总统特朗普随即签署通过《2020 财年国防授权法案》，对参与“北溪 2 号”项目的施工建设方实施制裁，但美国的这一举动遭到德国的强烈反对。

美国此举是出于地缘政治和经济利益考虑。因为美国希望对欧洲出口液化天然气，如果“北溪 2 号”项目顺利实施，美国在欧洲的液化天然气市场将被俄罗斯取代，美国的经济利益将受损，美国在欧洲事务上的话语权也会降低。

2.通过出口管制禁令达到瘫痪乃至切断供应链的效果以实现对企业的极限施压

发布出口管制禁令，达到瘫痪乃至切断供应链的效果，继而实现对目标企业的极限施压，是美国维护其经济霸权的第二种常见手段。美国一方面通过《出口管理法》（EAA）、《武器出口管制法》（AECA）和《国际突发事件经济权力法》（IEEPA）等国内出口管制法律对军用产品、军民两用产品以及技术的出口进行管制，另一方面又通过《瓦森纳协定》联合盟友和主要西方国家对军用产品、军民两用产品和高技

术产品向中国等国家的出口实行控制。

二战后美苏冷战时期，为防止苏联阵营发展高端武器，在美国提议下，美国、英国、日本、法国、澳大利亚等 17 个国家于 1949 年 11 月在巴黎成立了巴黎统筹委员会（简称“巴统”），限制成员国向社会主义国家出口战略物资和高技术。苏联解体后，巴统于 1994 年 4 月 1 日正式解散。2 年后，以美国为主导的《瓦森纳协定》在奥地利维也纳签署，继承了巴统的禁运政策。该协定成为美国对异己国家高技术产业发展进行围堵和打压的重要手段。通过出口管制禁令瘫痪乃至切断供应链的方法常常在其他国家企业威胁到美国的技术领先优势时被使用，典型的案例是日本“东芝事件”和欧洲“空客公司监听案”。

美国和日本在 20 世纪 80 年代在高新技术领域竞争激烈，1987 年，东芝集团旗下的东芝机械被揭露偷偷向苏联出口降低潜艇噪音的数控机床。随后，美国发起了对东芝机械公司的调查以及对日本的经济制裁。如表 1 所示，1985 年美国半导体协会（SIA）向美国贸易代表办公室（USTR）提起有关日本半导体企业倾销的诉讼，由此美国对日本电子产品发起了 301 调查。1986 年美国与日本签订《美日半导体协议》，要求约束日本的倾销行为，限制日本半导体对美国的出口，并鼓励日本将美国半导体产品的市场份额增至 20%。1991 年第一个为期五年的《美日半导体协议》到期，美日又签订了第二个五年协议，同时进一步扩大美国半导体产品在日本的市场占有率。之后，美国半导体企业逐渐恢复市场竞争力，于 90 年代中期超越日本半导体企业

的全球市场占有率。

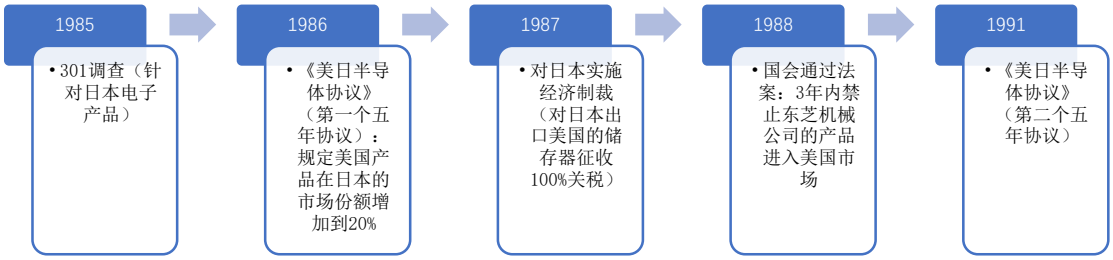

表 1：“东芝事件”后美国对日本的调查与制裁

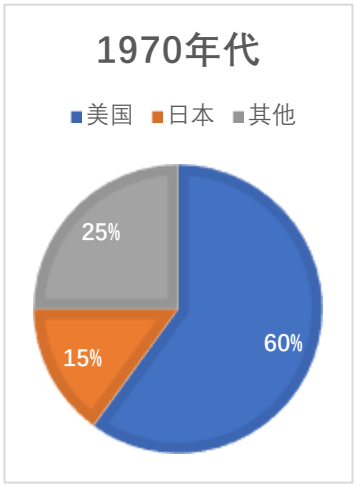

图 2.1：美日半导体产品占世界市场份额（1970 年代）

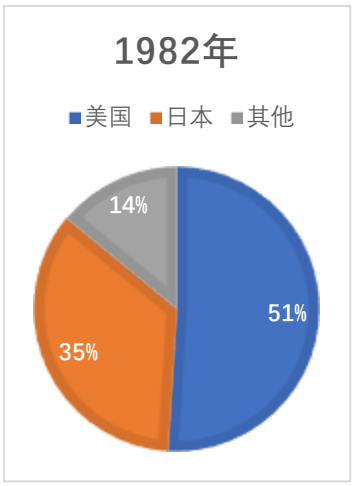

图 2.2：美日半导体产品占世界市场份额（1982 年）

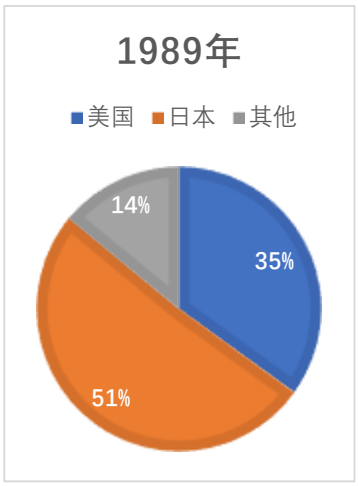

图 2.3：美日半导体产品占世界市场份额（1989 年）

图 2：美日半导体产品占世界市场份额变化[3]

“东芝事件”表面上看是一起由违反巴统出口管制规则而引起的美日贸易摩擦，但日本东芝机械公司并不是唯一的交易方，挪威国营军工企业康斯伯格公司也牵涉其中，两家公司联手完成对苏联的数控机床出口。双方的合作使得这一违反出口管制的问题成为多国贸易问题，但美国却将矛头直指东芝机械公司。这表明美国的意图绝不仅仅是为了维护巴统的禁运协议，更是为了保住自身在高新技术产业的领

[3] “The U.S.-Japan Semiconductor Agreement: Keeping Up the Managed Trade Agenda”, *The Heritage Foundation*, January 24,1991, https://www.heritage.org/asia/report/the-us-japan-semiconductor-agreement-keeping-the-managedtrade-agenda.

先地位。作为核心战略产业，半导体产业是衡量一国科技领导力的重要指标。如图 2.1 所示，在上世纪七十年代，美国的半导体产业在世界范围具有绝对统治力，在世界市场中占有 60%的份额，而当时日本半导体产业远远落后于美国，其世界市场占有率约为 15%。进入上世纪八十年代后，日本的半导体产业飞速发展，到 1982 年已占有 35%的世界市场份额，威胁了美国在半导体产业的统治地位。1983 年美国商务部的报告指出，在五大高新技术领域中，美国目前只在飞机制造、航空航天技术领域仍然保持着领先地位，而在半导体技术、光纤技术、智能机械技术领域落后于日本。[4]美国自二战以来建立起的经济霸权需要通过自身在高新技术领域的领先实力来护持。日本半导体产业在上世纪八十年代的飞速发展挑战了美国在先进技术上的领导力，因而受到美国的调查与制裁，被迫通过与美国签订半导体协议的方式，一方面减少对美的半导体产品出口，一方面保证美国半导体企业的在日本的市场份额。这些行为背后反映了美国对自身经济霸权的护持，尤其是面对自身技术优势的相对衰落时，美国通过加征关税和签署协议等方式，限制日本电子产品的出口和半导体产业的发展。美国就“东芝事件”对日本展开贸易调查与经济制裁的时间线，正与日本半导体产业腾飞的时间脉络重合，由此可以窥见美国在“东芝事件”背后的真实意图。

需要指出的是，美国对日本半导体行业的打压方式，就是摧毁日本半导体行业的成品制造能力（当时是内存条为代表的成品），然后

[4] 侯文富：《“东芝事件”及其影响刍议》，《日本学刊》2000 年第 1 期，第 46 页。

迫使日本转向配件化的制造业上端移动，生产诸如光刻胶之类的配件。这种移动看似伴随技术进步，但在国家层面上意味着日本以及日本相关企业在全球产业体系中的地位被大幅度边缘化，失去了自主性，只有在配合美国的产业链封锁或者排挤战略时，才能真正发挥实质性的作用，否则只能在日韩之间的有限度争端中起到有限度的作用。

更极端的实践，则是美国企业与政府联合在商业行为中表现出的非商业化实践模式。1994-1995 年间，在沙特阿拉伯价值 60 亿美元的飞机合同竞标中，欧洲空中客车公司输给了美国波音公司。由于怀疑内部存在不公平竞争，空客公司随后向欧盟发起投诉，欧盟遂成立临时委员会着手调查。结果发现波音公司为“五眼联盟”提供了一套名为“梯队（Echelon）”的全球电子监控系统，美国国家安全局利用该系统的电信卫星拦截功能，从一架商业通信卫星上获取了欧洲空客公司与沙特政府、航空公司之间所有的传真和电话。美方通过分析通讯内容，认为空客公司的代理商向沙特官员行贿，并将大量商业机密提供给美国波音公司，从而推动了美国波音和麦克唐纳·道格拉斯公司的竞标并最终成功。有趣的是，在以欧洲空客案为代表的美国监听商业机密的案件中，所有的受害公司或个人却被美方称为“犯罪者”，冠之以商业贿赂、非法转让、窃取专利等罪名。而且，临时委员会的报告还发现，美国开展商业监听帮助美企获得竞争优势的类似案例还有许多，仅公开可查的就有 20 多起，覆盖日本、法国、德国、以色列等国的多家著名企业。但更令人震惊的是，在事情暴露之后，曾经出任美国中央情报局局长的伍尔西居然在《华尔街日报》上公开发表

题为“为何要监听盟友”的署名文章，**将这种监听行为定义为“美国企业获得公平贸易环境的必要条件。”**

总之，欧洲空客公司案体现了美国“双重标准”的霸权逻辑：即美国拥有最先进的技术，因此在各类商业竞标中获胜是理所应当的；而欧洲在技术、成本、质量、市场等方面落后于美国，若欧洲企业战胜美国公司，那么一定是该国或该公司采取了贿赂等非法手段。换言之，只有美国在技术、经济、社会等领域占据绝对优势的世界，才是真正“公平合理”的世界。这条逻辑线与如今美国对华经济施压如出一辙。

3.利用国内法律程序、长臂管辖和实体清单等对企业进行打压

全球化导致全球各国深度相互依赖，但这种依赖具有不对称性。这为国际关系中复杂相互依赖中的优势一方带来了权力，即这种非对称性可被用于逼迫对象国改变其政策行为，服从施压国意志。[5]作为世界唯一的超级大国，美国为维护其经济霸权经常采取的第三种手段是利用其国内法律程序、长臂管辖和实体清单等对企业进行打压。自 20 世纪 80 年代以来，这种打压主要面向日本和欧洲企业。

日本计算机产业在上世纪 70 年代迅速崛起，威胁到美国原有的主导地位，1982 年，美国联邦调查局（FBI）线人谎称拥有 IBM 计算机最新技术，使用钓鱼执法的招数，诱使日本日立与三菱电机的员工出钱购买。等两公司拿到相关图纸后，FBI 迅速逮捕了 6 名“商业间谍”，还对 12 名日本员工发出通缉令。日立和三菱电机不得不与 IBM

[5] 徐飞彪：《美长臂管辖的起源、扩张及应对》，《中国外汇》2019 年第 14 期，第 34 页。

缔结了技术使用费的支付合同，仅 1983 年，日立公司就支付了约 100 亿日元。

近十几年来，美国司法部在反海外腐败、违反制裁的伪装下，通过起诉欧洲高科技公司的高管，给公司开出高额罚单的手段，成功打击甚至瓦解了欧洲多个大型跨国公司。

作为法国的工业明珠，阿尔斯通公司（Alstom）曾在水电设备、核电站常规岛、环境控制系统、交通运输部超高速列车和高速列车等领域均位列世界第一，并在城市交通市场、区域列车、基础设施设备以及所有相关服务位居世界第二。此外，阿尔斯通公司在能源相关领域也表现强劲，它提供了占世界装机总容量 15%的设备，在运输和输配电市场等相关领域也位列世界第二。

2013 年的时候，阿尔斯通已被美国司法部调查 3 年多，但当时阿尔斯通首席执行官柏珂龙决定不与美国当局合作。为了达到削弱和制裁阿尔斯通的目的，美国联邦调查局于 2013 年在美国机场抓捕了前阿尔斯通高管皮耶鲁齐，之后他被起诉入狱。美国司法部指控皮耶鲁齐涉嫌商业贿赂，并对阿尔斯通处以 7.72 亿美元罚款。[6]当看到皮耶鲁齐被抓之后，阿尔斯通公司人心惶惶，阿尔斯通高管开始与美国司法部全面合作。为了自保，首席执行官背着法国政府及阿尔斯通管理层的大部分人，通过秘密协商，将包括电力在内的公司四分之三业务卖给美国通用电气公司。尽管欧盟随后介入，但美国仍然成功收购

[6] U.S. Department of Justice, “Alstom Pleads Guilty and Agrees to Pay $772 Million Criminal Penalty to Resolve Foreign Bribery Charges”, December 22, 2014, https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery.

阿尔斯通，并获得维护所有法国核电站的权力，这些核电站提供法国75%的电力。这一收购也改变了全球能源设备行业的竞争结构，美国通用电气公司、德国西门子公司、瑞典通用电气布朗-博韦三家企业呈现三足鼎立之势。

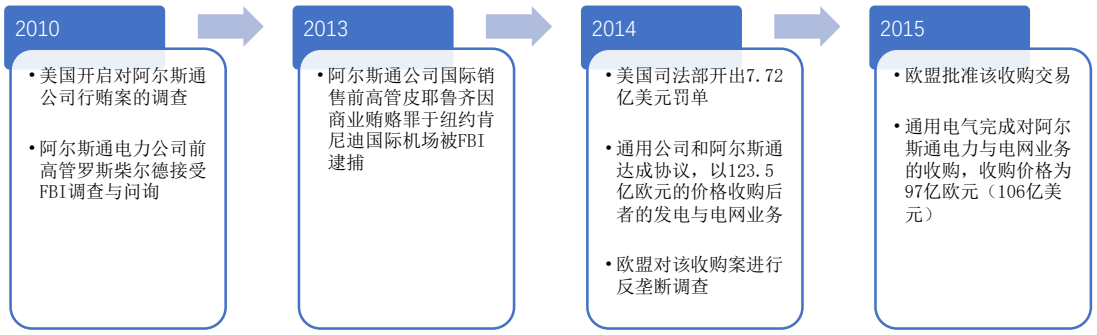

表 2：“阿尔斯通行贿案”时间线

据统计，在 1977 至 2014 年间，涉及美国《反海外腐败法》的调查中，30%（474 项）是针对非美国企业的，但它们支付的罚款占总额的 67%；在被美国罚款超过 1 亿美元的 26 家企业，仅有 5 家是美国企业，21 家非美国企业中 14 家是欧洲企业。如图 3 所示，截止目前，在所有被处罚的前十名的企业中，没有一家是美国本土企业。

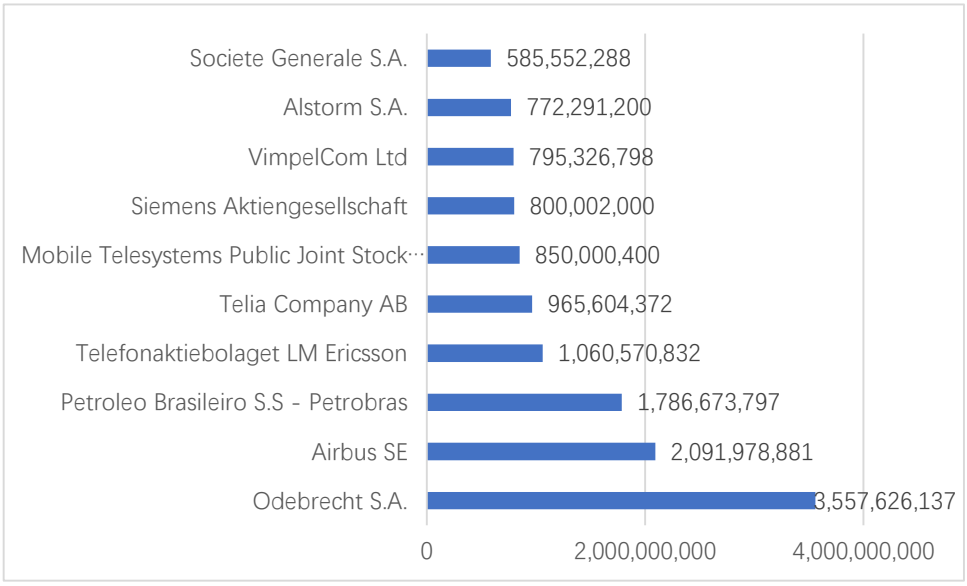

图 3：美国《反海外腐败法》罚款排名前十的公司（单位：美元）[7]

[7] Source: Largest U.S. Monetary Sanctions by Entity Group, Stanford Law School Foreign Corrupt Practice Act

由此可见，包括盟友在内，任何挑战美国经济霸权的企业甚至整个国民经济都会受到美国严厉的打压和制裁。而近些年来，随着发展中国家和新兴市场经济体的崛起，美国利用国内法律程序、长臂管辖和实体清单等对相关国家和经济体企业进行打压的案例也在不断上升。

《特别 301 报告》是美国贸易代表办公室公布的关于世界各国的知识产权保护的年度报告。自 1989 年以来，美国已经发布到近 30 份《特别 301 报告》。报告涉及的国家数字逐年增多，从 1989 年的 25 个增加到 1998 年 70 个；针对的国家也从过去以发达国家和部分发展中国家为主转变为以发展中国家和新兴经济体为主；所涉及的议题也逐渐超出知识产权的范围，涵盖反腐、环境和公共卫生等内容。美国通过发布《特别 301 报告》，借助其霸权地位，采取单方面设定标准、单方面发布报告、单方面解释、单方面调查、单方面制裁的高压方式迫使相关国家屈从，进而巩固美国在知识产权领域以及贸易投资领域的优势地位。此外，《特别 301 报告》还是美国在与相关国家谈判时的重要筹码，美国通过掌握话语权，占领道德高地，迫使其他国家在相关领域对美国作出让步。

三、美国坚持使用传统金融、技术和法律手段维护其数字霸权

从传统经济霸权到数字霸权的建立，尽管美元支付体系目前已经受到冲击，但依然处于主导地位，美国仍然利用金融工具打压数字领

Clearinghouse, http://fcpa.stanford.edu/statistics-top-ten.html.

域的竞争企业，也防范数字支付产业对美元支付体系的进一步冲击；在技术和供应链层面，虽然新兴国家不断崛起，个别国家逐步实现产业升级，爬升到产业链的顶端，但美国及其技术已经完全渗透融合到全球供应链各个角落，使得美国采取绝对的禁令对相关企业进行打压成为可能；最后是法律和国际制度，目前围绕数字经济的国际规则缺失，大国在跨境数据流动和技术贸易领域争端频频，WTO 几乎处于失灵状态，美国频繁使用国内法律和行政命令，以国家安全为由制裁打压竞争者，并试图塑造美国主导的全球数字产业和生态。

1.通过将合规武器化压制他国企业发展

作为第一款真正意义上成功赢得国外用户青睐的中国社交产品，TikTok 自 2018 年起在全球每月活跃用户达 5 亿，成为苹果 App Store 上下载量最多的应用程序。然而自 2019 年以来，美国大肆渲染 TikTok 的安全威胁，使其在全球范围内面临困境。美国先是指控 TikTok 母公司字节跳动与中国政府共享数据，随后又称 TikTok 通过内容审查压制言论。此外，美国一直寻求将合规问题武器化，以应对 TikTok 在全球范围内的崛起。**这里的武器化，就是首先从技术层面入手，就所谓个人隐私信息收集、跨境数据传输、内容审查机制、与中国政府关系等看似技术化、程序化的细节问题，对 TikTok 进行审查；在发现 TikTok 逐一在形式、程序以及操作层面化解这些技术性的议题之后，直接使用“疑似威胁国家安全”的“口袋”**，以不容 TikTok 回应和辩护的方式，开展极限施压行动：

先是对 TikTok 进行安全审查，随后又在联邦机构中发布针对

TikTok 的下载禁令。最近，美国更是直接通过行政令的方式要求美国资本对 TikTok 进行强制收购。美国的这种做法打破了公平竞争的格局，使得美国传统社交巨头得以以非正常方式获得市场，也会引起外界对于美国市场经济地位的质疑。

2.以技术管控、出口禁令等方式对企业实施精准打压

以技术管控、出口禁令等方式对企业实施精准打压，以大疆和华为案为典型。世界上最大的民用无人机制造商大疆创新，是中国一家以生产、研发民用无人飞行载具及航空摄影系统为主的科技公司。该公司生产的无人机产品获得了全世界航拍、摄影爱好者的喜爱，占有全球 70%的市场。然而自 2017 年起，美国政府便寻找各种理由对其无人机产品进行打压。美国海关官员在一份报告中称，官员们有“适度的信心”认为，大疆的商用无人机和软件“正在向中国政府提供美国主要基础设施和执法机构的数据”。2019 年 5 月 20 日，美国国土安全部以用户信息安全问题为由将大疆作为打击目标。10 月，一部分议员提出立法，要求禁止所有联邦机构使用在中国制造或组装的无人机。11 月，美国内政部宣布，停飞其机队中所有中国制造、或含有中国制造零部件的无人机。就市场地位和产品质量而言，由于目前尚无无人机厂商能够完全取代大疆，因此美国政府反复寻找技术管控措施遏制大疆发展。尽管作出诸多改变，大疆仍面临美国压力。美国方面仍可能突破目前技术管控措施，采取行政手段打击大疆，例如进一步将大疆列入实体清单从而禁止美国公司与其直接往来。

2018 年 8 月，特朗普签署美国《2019 财年国防授权法案》，该法

案第 889 条要求，禁止所有美国政府机构从华为购买设备和服务。随后，美国对华为的打压不断升级，美国将华为列入商务部“实体清单”，禁止美国企业向华为出售芯片。2020 年 5 月 15 日，美国商务部宣布将通过限制华为使用美国技术和软件在国外设计和制造其半导体的能力，来保护美国的国家安全。此次出口规则改变后，使用美国芯片制造设备的外国公司在向华为或海思等附属公司供应某些芯片之前，都将被要求获得美国许可证。2020 年 8 月 17 日，美国进一步收紧对华为的限制，禁止供应商在未取得特别许可的情形下贩售使用美国技术制造的芯片给华为，把 5 月出台的制裁措施的潜在漏洞给堵住，这些漏洞让华为可以通过第三方取得相关技术。美国一方面希望通过对华为实施断供，阻止其技术发展；另一方面又试图阻止其他国家采购华为的 5G 设备。

美国滥用国家力量，对华为进行无底线的封锁和打压的行为是典型的霸权主义行为。而且，从产业角度看，根据 BCG 相关报告，中美贸易紧张局势或将造成两国半导体技术产业脱钩，美国半导体收入将下降 37%；如果按 2018 年收入计算，相当于减少 830 亿美元。其中约四分之三的影响将是由于中国客户因美国技术出口禁令而不得不更换美国半导体产生的直接后果。可见，美国此举违背了产业客观规律，将给全球产业发展造成严重伤害。

3.利用重新制定国际规则的能力优势挤压盟友的合理利益

2019 年 12 月 10 日，美国、墨西哥和加拿大签署了修订后的《美墨加协议》（USMCA），取代已有 25 年历史的《北美自由贸易协定》

（NAFTA），并于 2020 年 7 月 1 日正式生效。

自 2017 年起，美国政府多次批评《北美自由贸易协定》造成美国制造业流失，并以退出协议为由要求重新谈判。因此，修订后的《美墨加协议》被视为特朗普总统执政期间的主要政绩之一，甚至被美国政府标榜为“21 世纪最高标准的贸易协定”。然而，《美墨加协议》中的许多条款却再一次体现了美国的数字霸权。因为该协议不仅扩大了数据跨境流动的范围，增加了禁止个人数据本地化的强制性和约束力，还将这一限制延伸至金融领域，可以方便美国金融监管机构通过履行监管职责获取墨西哥和加拿大的金融数据。

谷歌、脸书、苹果、亚马逊在多国从事经营、获取巨额收入，却选择低税率地区注册总部以求“合法”避税，使所在国传统产业和中小型技术企业遭受不公平竞争，使用户所在国政府蒙受损失，这让法国、意大利等欧盟成员国不满。2018 年 3 月，欧盟委员会公布立法提案，任何一个欧盟成员国均可对发生在其境内的互联网业务所产生的利润征税。实现互联网企业公平缴税是全球性的议题，任何单个国家都无法自行解决。在法国提出征收数字税后，美国立马宣布将对法国加征关税作为反制。而在 2020 年 6 月，美国又以疫情为由退出在经济合作与发展组织框架下就征收跨国技术企业数字税协议开展的谈判。以上案例都反映出美国在国际谈判中凭借强势地位，利用国际规则漏洞获取不公平优势。

四、清洁网络计划是新形势下美国实现其数字霸权的重要尝试

2020 年 4 月 29 日，美国国务卿蓬佩奥宣布，美国国务院将开始要求为所有进出美国外交设施的 5G 网络流量实行 5G 清洁路径计划，要求禁用一切被认为“不可信”的 IT 供应商（包括中兴和华为）通过包括传输、控制、计算或存储设备在内的方式接入任何国家和运营商的 5G 网络。该计划被纳入 2020 年 6 月推出的清洁网络计划（Clean Network）当中。随后，美国又在 2020 年 8 月 5 日更新清洁网络计划，在 5G 清洁路径计划的基础上推出了五项新的计划来保护美国的关键电信和技术基础设施。至此，“清洁网络”计划基本覆盖全供应链生态闭环，旨在为了防止所谓中国互联网企业对美国主导的互联网世界形成颠覆，最终维护美国的数字霸权，**这是第一次美国在实体层面不具备产业意义上的压倒性优势的情况下，主要依托产业和技术之外的手段，践行网络霸权的重要尝试。**

1.清洁网络计划本质上是一种以供应链安全为由设置的非关税壁垒

随着中国在以 5G 为代表的先进网络信息技术和数字经济发展方面取得领先，美国国内开始盛行所谓“红色技术威胁”或是“数字东方主义”的论调。其本质是以一种二元对立的视角来叙述凡是中国的信息技术一定是用于监控和国家安全目的，凡是中国的数字经济应用一定存在隐私泄露的问题，凡是中国在技术研发或经济发展中取得的成就一定是靠包括网络窃密和违法市场经济规则等不正当手段获得的。这套政治说辞不仅能够最大限度凝聚美国民众乃至整个西方世界对古老东方神秘国度的忧惧，激发民族主义情绪，而且能够为西方主

要发达国家在技术上的衰落和经济上的凋敝开脱责任，并重新凝聚西方民众对自身文明和制度的认同。

“清洁网络”计划声称要从电信服务、程序商店、应用软件、云服务、电缆以及 5G 等方面全方位排斥中国信息产业产品及服务。该计划带有浓厚的主观色彩，其对“清洁”的定义充斥着意识形态偏见，即只要不是中国供应商就是“清洁”的，只要是美国看不惯的就是“不清洁”的。但是，美国对于所谓“清洁”的判定不是对技术进行客观判定，而是以技术来源方的身份属性作为主要判定标准。因此，清洁网络计划可被视为美国从全供应链角度对中国网络产业精准打压，本质上是一种以供应链安全为由设置的非关税壁垒。

2.清洁网络计划构成美国实现其数字霸权的一整套政策工具箱

2020 年 6 月，美国提出清洁网络计划，包括通过制订清洁网络名单，采取综合措施保护美国公民的隐私和公司敏感信息免受所谓中国等恶意行为者的侵扰。如图 4 所示，该计划于 8 月 5 日更新，在 5G 清洁路径计划的基础上推出了五项新的计划来保护美国的关键电信和技术基础设施。清洁网络的五项新工作包括：清洁运营商，确保所谓不受信任的中国运营商不与美国电信网络连接；清洁商店，从美国移动应用商店中删除不受信任的应用；清洁应用程序，防止所谓不受信任的中国智能手机制造商在其应用商店中预装（或以其他方式使之可供下载）受信任的应用程序；清洁云，防止美国公民敏感个人信息和企业知识产权在百度、阿里巴巴、腾讯等可被外国对手访问的基于云的系统上进行存储和处理；清洁电缆，确保连接美国与全球互联网

的海底电缆不被所谓中国大规模破坏并进行情报收集。“清洁网络”计划基本覆盖全供应链生态闭环，是美国在对中国网络产业长期研究和深度解剖基础上提出的精准打击策略，可以看作是实现其数字霸权的一套工具箱。美国动用国家力量采取单边行动对中国企业进行围堵，目的是为了防止中国互联网企业对美国主导的互联网世界形成颠覆，最终目标仍是维护美国的数字霸权。

图 4：清洁网络计划

3.清洁网络计划将损害其他国家的数字主权，阻碍行业发展

清洁网络计划在实现美国数字霸权的过程中，将损害其他国家的数字主权。首先，每个国家都有自主选择自己的可信供应商和可信服务的自由，而清洁网络计划将剥夺相关国家的这一自由。其次，美国通过清洁网络计划，将电信运营商、移动应用程序、移动应用商店、云服务、电缆和 5G 供应商均纳入其管控之中，这种管制泛化将侵犯各国网络运营和监管的自主权。最后，数据作为重要的国家资产，有必要加强本地储存和业务本地监管，而美国出台《云法案》对数据等进行长臂管辖将严重损害相关国家的数据自主权。

需要说明的是，美国的这种实践网络霸权的尝试，在传统上支持和赞同美国以非对称方式治理全球网络空间的社群以及持经典自由

主义立场的学者那里，也引发了强烈的反对：

佐治亚理工学院教授、互联网治理项目的创始人弥尔顿·穆勒（Milton Muller）认为，“美国推行清洁网络计划的目标是使中美之间的互联网和全球信息社会分离，并使中国脱离信息经济。但是这种做法可能伤及美国自身，因为世界其他国家可能会效仿美国，对苹果、谷歌、脸书和推特等美国互联网公司采取类似的措施。而且，特朗普以泛化的国家安全为理由对中国公司采取措施，认为这样就可以阻止中国的发展，这是不现实，也极其不明智的。”[8]信息技术与创新基金会副总裁丹尼尔·卡斯特罗（Daniel Castro）认为，“美国在声称使用外国公司的技术有内在的国家安全风险时应该谨慎，因为如果其他国家依据同样的逻辑，美国技术公司也将被排除在外国市场之外，这种做法将带来互联网碎片化的严重风险。”[9]

五、化解清洁网络计划风险的建议

美国在网络空间构建的是一种支配型的秩序，这种支配型的秩序要保证美国处于压倒性的优势位置。这种压倒性的优势位置具体体现在四个方面：第一，客观上美国要处于安全状态；第二，美国要求在网络空间具备非对称的行动自由；第三，要求美国企业和产业在全产业处于压倒性的领先位置，不允许看不惯的任何企业占据这个位置，即使是盟友的企业也不例外；第四，它在战略上基本不考虑全球化以

[8] Rob Lever, “Trump moves on China apps may create new internet 'firewall'”, Tech Xplore, August 7, 2020, https://techxplore.com/news/2020-08-trump-china-apps-internet-firewall.html

[9] Ibid.

及具体的、内生的产业分工的合理需求，带有很强的意识形态和主观色彩。这样一种支配型的秩序会严重扰乱全球市场，给产业和世界各国利益造成严重损害。而清洁网络计划作为一种以供应链安全为由设置的非关税壁垒，违背产业发展客观规律，将损害其他国家的数字主权，阻碍行业发展。因此，国际社会应该团结起来，为行业营造公平的竞争环境、制定客观公正的标准并采取有效措施建立信任，化解清洁网络计划带来的风险。

1.保持开放的市场，为 ICT 供应商创造公平的竞争环境，避免设置贸易壁垒

针对美国以国家安全为由将中国企业列入“实体清单”的做法，2019 年 5 月 31 日,中国商务部宣布将建立“不可靠实体清单”制度，对美国企业、协会等实体进行反制。作为世界第二大经济体，中国与世界各国，尤其是欧盟，拥有广泛的经济往来。自 1975 年 5 月中国与欧洲经济共同体正式建立关系，中国与欧盟先后建立了合作伙伴关系、全面伙伴关系和全面战略伙伴关系。目前，欧盟已经连续 16 年成为中国最大的贸易伙伴，双方有着广泛的共同利益。因此，欧洲国家应该保持开放的市场，为中国 ICT 供应商创造公平的竞争环境，避免以国家安全为由设置非关税壁垒。只有这样，才能在与中国的经济来往中实现共赢，不会因对中国企业的歧视性对待遭遇中国反制。

2.根据国际标准和方法建立采购惯例和准则

具有国际影响力的高水准全球 ICT 认证和测试合规项目可以提高 ICT 的安全性和可信度。建立一套合规项目，并由现有或新的全球

机构运行和实施，为客户和利益相关者提供遵守标准和最佳实践准则的客观依据，将极大地降低相关技术安全检测和应用成本。国际社会应该共同努力，制定基于技术的中立且无歧视的国际标准，以客观的标准，和明确告知风险且高度透明的要求作为依据，建立采购惯例与准则，反对基于主观判断、以自我为中心的歧视性标准，在以 5G 建设为代表的信息产业发展中为本国获取最具性价比的全球化资源，实现本国利益的最大化。

3.建立全球 ICT 供应链安全规范，并采取有效措施建立信任

欧盟网络和信息安全局（ENISA）于 2012 年发布《供应链完整性—ICT 供应链风险和挑战概览，以及未来的愿景》报告，并于 2015 年更新。除提供可供 ICT 供应链相关参与者借鉴的实践做法外，该报告还建议公私合作设立国际评估框架，以有效评估 ICT 供应链风险管理。中、俄等国在 2011 年和 2015 年两度向联合国提交的《信息安全国际行为准则》中，也就确保 ICT 供应链安全提出了具体倡议，强调应“努力确保信息技术产品和服务供应链的安全，防止他国利用自身资源、关键设施、核心技术、信息通讯技术产品和服务、信息通讯网络及其他优势，削弱接受上述行为准则国家对信息通讯技术产品和服务的自主控制权，或威胁其政治、经济和社会安全”。[10]这些都是比较好的做法，有助于在各国之间以及企业和客户之间建立信任，促进行业的良性发展。

[10] 吕晶华:《ICT 供应链安全国际治理制度体系分析》,《信息安全与通信保密》2020 年第 4 期，第 26 页。

附录 1：欧洲“梯队”系统临时委员会公开案例

案件	机构	时间	内容	手段	目标	后果
法国航空（Air France）	DGSE	到 1994 年	出差商人之间的对话	在法航飞机的头等舱中发现了漏洞，该公司随后向公众道歉	获取信息	不详
空客（Airbus）	NSA	1994 年	空客与沙特阿拉伯国家航空公司之间签订的飞机订单信息	拦截谈判双方之间的传真和电话	将信息转发给空中客车公司的美国竞争对手波音和麦克唐纳-道格拉斯	美国人赢得了合同（60 亿美元）
空客（Airbus）	NSA	1994 年	与沙特阿拉伯价值 60 亿美元的合同	通过电信卫星拦截空客公司与沙特阿拉伯国家政府、航空公司之间的传真和电话	揭发贿赂	空客公司的美国竞争对手麦克唐纳-道格拉斯赢得了合同
巴斯夫（BASF）	Marketing manager	不详	巴斯夫化妆品部门生产护肤霜原料的方法	不详	不详	由于被发现而未果

德国联邦经济事务部（Federal German Ministry of Economic Affairs）	CIA	1997 年	联邦经济事务部持有的有关高科技产品的信息	通过代理人	获取信息	特工暴露并被驱逐出境
德国联邦经济事务部（Federal German Ministry of Economic Affairs）	CIA	1997 年	通过爱马仕对伊朗的出口贷款，建立了向伊朗供应高科技产品的德国公司	中情局特工伪装成美国大使与负责阿拉伯地区的联邦经济事务部部长对话	获取信息	政府人员与德国安全部门取得联系，后者通知美国反对中情局的行动。中情局特工随后撤回
达沙（Dasa）	Russian Intelligence Service	1996 年 - 1999 年	购买和递交慕尼黑军火公司草拟的有关军备的文件	2 名德国人为俄罗斯政府工作	获取有关制导导弹、反坦克和防空导弹武器系统的信息	没有造成严重的军事后果，但导致了一定的经济损失
禁运（Embargo）	FIS	1990 年左右	恢复西门子对利比亚的技术出口禁运	监听电话	发现非法武器和技术转让	没有特别后果，没有阻止交货
爱纳康（Enercon）	Oldenburg 风力发电专家和 Kennetech 员工	不详	爱纳康公司在 Auirch 开发的风力发电厂	不详	不详	不详

爱纳康（Enercon）	NSA	不详	东弗里西亚的工程师 Aloys Wobben 开发的发电风轮	不详	将 Wobben 风轮的技术细节转发给一家美国公司	美国公司在 Wobben 之前获得了风轮专利，侵犯专利权
爱纳康（Enercon）	美国公司 Kenetech Windpower	1994 年	高科技风力发电厂从开关装置到风帆设计等重要细节	拍照	在美国成功申请专利	爱纳康放弃了进军美国市场的计划
爱纳康（Enercon）	Oldenburg 工程师 W.和美国公司 Kenetech	1994 年 3 月	爱纳康开发的 E-40 型风力发电机	工程师 W.传递细节，Kenetech 员工为工厂和电气组件拍照	NSA 员工表示，Kenetech 以爱纳康公司非法获取商业机密为由，对爱纳康侵犯专利权发起法律诉讼并搜集证据。据 NSA 员工称，有关信息已通过“梯队”系统传递给 Kenetech。	不详
爱纳康（Enercon）	美国公司 Kenetech Windpower	1996 年前	爱纳康风力发电厂的相关数据	Kenetech 工程师为工厂拍照	Kenetech 复制工厂	证明爱纳康无罪；针对间谍采取法律行动；约

						损失几亿马克
日本贸易省（Japanese Trade Ministry）	CIA	1996 年	关于日本市场上美国汽车进口配额的谈判	入侵日本贸易省的计算机系统	让美国谈判代表 Mickey Kantor 接受降低报价	Kantor 接受最低报价
日本车（Japanese cars）	US Government	1995 年	关于日本豪华车进口的谈判；日本汽车排放标准信息	通讯情报，暂无详细信息	获取信息	不详
洛佩斯（López）	NSA	不详	大众公司和洛佩斯的视频会议	以不良行为拦截	将信息转发给通用汽车公司（General Motors）和欧宝公司（Opel）	据称，拦截行动为国家检察署提供了“非常详细的证据”以进行调查
洛佩斯（López）	洛佩斯及其三位员工	1992 年-1993 年	计划、制造和购买的文件和信息，特别是西班牙工厂的相关文件，包括各种型号的成本信息、项目研究、购买和保存策略	收集资料	大众公司使用通用汽车文件	庭外和解：1996 年，洛佩斯辞去大众汽车公司总经理的职务，向通用汽车和欧宝公司汽车支付了 1 亿美元律师费，并在 7 年中里共购买 10

						亿美元的备件。
洛佩斯（López）	NSA	1993 年	José Ignacio López 与大众汽车老板 Ferdinand Piëch 之间的电视会议	录制视频会议并将其转发给通用汽车公司	保护通用汽车公司在美国持有的商业秘密，洛佩斯希望将价格表、新车工厂和新小型车的秘密计划发送给大众公司	洛佩斯的身份暴露，1998 年停止刑事诉讼以交换罚款；对 NSA 没有影响
洛斯阿拉莫斯（Los Alamos）	Israel	1988 年	以色列核研究计划的两名雇员入侵洛斯阿拉莫斯核武器实验室的核心计算机	黑客	获取有关美国原子武器起爆装置的信息	黑客逃到以色列，一人在以色列被短暂拘留，与以色列特勤局的联系尚未得到正式确认
走私（Smuggling）	FIS	二十世纪 70 年代	将计算机走私到 GDR 中	不详	发现向 Eastern Bloc 的技术转让	没有特别的后果，没有阻止交货

法国高速列车（TGV）	DGSE	1993 年	西门子成本计算；向韩国提供的高速列车合同	不详	较低的报价	ICE 的制造商将合转让给 Alcatel-Alsthom
法国高速列车（TGV）	未知	1993 年	AEG 和西门子就政府向韩国提供高速列车的合同计算成本	西门子声称正在窃听其首尔办事处的电话和传真	英法竞争对手 GEC Alsthom 获得谈判优势	韩国决定支持 GEC Alsthom，尽管最初认为德国出价更优
汤姆森-阿尔卡特 v（Thomson-Alcatel v）；雷神（Raytheon）	CIA/NSA	1994 年	向法国汤姆森-阿尔卡特公司授予巴西亚马逊河流域卫星监测合同，价值 14 亿美元	拦截中标者的往来通信	揭露腐败	克林顿向巴西政府表达不满；在美国政府的压力下，合同被授予美国雷神公司
汤姆森-阿尔卡特 v（Thomson-Alcatel v）；雷神（Raytheon）	US Department of Commerce	1994 年	有关巴西雨林雷达监测的项目的谈判，价值数十亿美元	不详	获取合同	法国公司 Thomson CSF Alcatel 在竞标中输给了美国雷神公司

汤姆森-阿尔卡特 v（Thomson-Alcatel v）；雷神（Raytheon）	NSA；Department of Commerce		一项有关亚马逊盆地（SIVA）的监控项目，价值 14 亿美元项目的谈判；发现巴西竞标小组接受了贿赂。	监视 Thomson CSF 和巴西之间的谈判，并将调查结果转发给雷神公司。	揭露贿赂；合同中标	雷神公司赢得合同
蒂森（Thyssen）	BP	1990 年	北海天然气和石油钻探合同，价值数百万美元	拦截中标者（蒂森）发送的传真	发现腐败	BP 提起针对蒂森的损害赔偿诉讼
大众	未知	近几年	不详	通过无线电传输图像的红外摄像机	获取有关新发展的信息	大众公司承认利润损失总计数亿德克
大众	未知	1996 年	大众汽车测试的 Ehra-Lessien 电路	隐藏相机	有关新大众车型的信息	不详

表格来源：Temporary Committee on the ECHELON Interception System. REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)).2001.7.11.

附录 2：美国制裁和打压他国重点企业案例

案件	美方制裁机构	时间	内容及制裁方式	美方目标	后果
日立（HITACHI）；三菱电机（Mitsubishi Electric Corporation）	联邦调查局（FBI）	1982-1983 年	FBI 线人谎称拥有 IBM 计算机最新技术，使用钓鱼执法的招数，诱使日本日立与三菱电机的员工出钱购买。	保护美国在计算机领域的主导地位	FBI 迅速逮捕了 6 名“商业间谍”，还对 12 名日本员工发出通缉令，日立和三菱电机不得不与 IBM 缔结了技术使用费的支付合同。仅 1983 年，日立公司就支付了约 100 亿日元
东芝（Toshiba）	美国半导体协会（SIA）；美国贸易代表办公室（USTR）	1981-1985 年	认为东芝机械公司存在对苏联的违规出口，发起对东芝机械公司的调查以及对日本的经济制裁	维护美国在高新技术产业的领先地位	东芝机械公司社长饭村和雄、董事长佐波正一和总经理杉一郎先后辞职，东芝公司承担美国取消相应合同订单的损失
阿尔斯通(Alstom SA)	美国司法部（DOJ）；联邦调查局（FBI）	2013 年	FBI 逮捕前阿尔斯通高管皮耶鲁齐，美国司法部指控皮耶鲁齐涉嫌商业贿赂，并对阿尔斯通	美国获得维护所有法国核电站的权力	阿尔斯通高管开始与美国司法部全面合作，将包括电力在内的四分

			处以 7.72 亿美元罚款		之三业务卖给美国通用电气公司
抖音（TikTok）	美国政府	2019-2020 年	渲染 TikTok 的安全威胁，以行政令要求美国资本对 TikTok 进行强制收购	打压中国企业的海外市场，尤其是美国市场	待定
大疆创新（DJ-Innovations）	美国政府	2017-2019 年	美国陆军禁止使用大疆无人机及相关软件系统；在“10 项全能无人机项目”中排除大疆	打压中国无人机技术产业	美国、加拿大等国仍在大量使用大疆公司生产的无人机，具体结果待定
华为（Huawei）	美国司法部（DOJ）；美国商务部（BIS）	2018-2020 年	美国将华为列入商务部“实体清单”，限制华为使用美国技术和软件，禁止使用美国的芯片	打压中国高新技术产业	待定
北溪 2 号（Nord Stream 2）	美国政府	2019-2020 年	美国总统特朗普签署通过《2020 财年国防授权法案》，对参与“北溪 2 号”项目的施工建设方实施制裁	保护美国在欧洲的液化天然气市场不被俄罗斯取代	遭到以德国为代表的欧洲国家的强烈反对，但美国持续发起阻扰并不断威胁，北溪 2 号项目的走向待定

商汤科技（SenseTime）	美国司法部（DOJ）	2019 年	美国政府将商汤科技列入“实体管制清单”	与中国争夺 AI 技术的领先优势	短期未受到明显影响
卡巴斯基（Kaspersky）	美国国土安全部（DHS）	2017-2018 年	美国国土安全部要求政府机构在 3 个月内替换卡巴斯基软件	怀疑卡巴斯基与俄方情报机构有关，同时计划把该公司挤出世界 IT 市场	由于卡巴斯基代码深入美国政府的计算机基础设施，实施难度大；该公司计划斥 1200 万美元将机构服务器和软件开发业务由莫斯科迁移到瑞士
西门子（Siemens AG）	美国政府	2018 年	美国政府以“两国关系”作为威胁，要求伊拉克总理阿巴迪放弃与西门子合作	加强美国在伊拉克的影响力	西门子将价值 150 亿美元的伊拉克电力系统重建工程让给美国通用电气公司
土耳其溪（TürkAkım）	美国政府	2019-2020 年	美国总统批准《2020 财年国防授权法案》，要求对土耳其溪项目实施制裁	美国企图扩大在欧洲的天然气市场，限制俄罗斯在欧洲的天然气市场份额	无明显影响，该工程于 2020 年 1 月顺利投产

爱立信（Telefonaktiebolaget LM Ericsson）	美国司法部（DOJ）；美国证券交易委员会（SEC）	2019 年	美国政府根据《反海外腐败法》，通过监听、间谍、搜查等手段开展对爱立信公司的调查	打压爱立信进军美国 5G 市场的举措	爱立信对行贿行为认罪，并同意支付超过 10 亿美元的罚款
三星（Samsung Group）	美国政府	2012-2016 年	美国法院列列出三星智能手机的永久性禁售机型：dmire、Galaxy Nexus、Galaxy Note、Galaxy Note 2、Galaxy S2、Galaxy S2 Epic 4G Touch、Galaxy S2 Skyrocket、Galaxy S3 和 Stratosphere	保护美国苹果公司专利	三星向苹果赔偿 5.48 亿美元；美国地方法官同意苹果提出的永久性禁售 9 款三星智能手机

表格来源：课题组自制

The Authors

Project Head:

Shen Yi, Professor at Fudan Development Institute, Director of the Fudan University Cyberspace International Governance Research Institute

Project Deputy Head:

Jiang Tianjiao, Assistant Professor at Fudan Development Institute, Assistant to the Director of the Fudan University Cyberspace International Governance Research Institute

Project Members:

Lei Ting, Research Assistant at the Fudan University China Institute for Cyberspace Strategy

Lu Bin, Research Assistant at the Fudan University China Institute for Cyberspace Strategy

Zhu Jiahao, Research Assistant at the Fudan University China Institute for Cyberspace Strategy

Gao Yu, Doctoral student at the Fudan University School of International Relations and Public Affairs

Gong Yunmu, Doctoral student at the Fudan University School of International Relations and Public Affairs

Contents

Summary

In June 2020, the United States State Department unveiled its Clean Network program, which consists of a series of comprehensive measures, including the establishment of a clean network list, to protect the US's sensitive corporate information and individual privacy from so-called malicious actors including China. On August 5, 2020, the Clean Network program was expanded with five new lines of effort based on the 5G Clean Path initiative to protect the US's critical telecommunications and technology infrastructure. The Clean Network program was designed to cover the entire telecommunications supply chain and ecosystem. It represents a sophisticated strategy from the United States, based on long-term research and in-depth analysis of its target, which they intend to use to crack down on China's Internet industry. The program can be viewed as a toolkit for achieving digital hegemony.

The Clean Network program challenges the endogenous norms of the global information industry without presenting practical and rational alternatives. It's based on a highly ideological and subjective strategy and addresses a complicated mix of needs that are inaccurately expressed. It is essentially a non-tariff barrier that nominally intended to promote security and stability in the global information industry supply chain by creating highly replicable and discriminatory market access controls based on country of origin and identity. The Clean Network program, together with other programs like the 5G Clean Path initiative, is one of the latest key measures the United States has taken to preserve and consolidate its digital hegemony (i.e. the extension and expansion of geopolitical and financial hegemony in the digital age).

The Clean Network program is the latest product of the US strategy for digital hegemony. It aims to asymmetrically pursue US dominance in the information field by disrupting the basic rules of the game for certain industries. Two of the program's goals include: (1) achieving short-term global 5G dominance through discriminatory and exclusionary policies, despite the fact such dominance would be unsustainable as the country lacks any industrial advantages in 5G; and (2) preventing China's Internet industry from overtaking US's as the dominant global digital industry in the mid- to long-term by relying on non-industrial and non-technological means as the US doesn't have an overwhelming advantage in real industry sense. Achieving both of these goals would preserve the US's digital hegemony.

Through the Clean Network program and similar measures, the US is using geopolitics, political suspicion, and other non-technical and discriminatory arrangements to achieve these goals. It labels normal commercial and industrial competitors as national threats and then circumvents industry norms to act against these threats. Such acts include but are not limited to subjective and arbitrary interpretation of objective standards and the disregard of conventions and tacit understanding in practice. This creates a significantly distorted market order centered on the United States with certain asymmetric predatory characteristics. These behaviors threaten global business rules and represent typical hegemonic characteristics of double standards, unilateralism, and self-centeredness.

It should be noted that many countries and their representative multinational companies have become natural competitors of the United States in the international market since the 1980s due to the nature of economic development and technological progress. Some have even threatened the US's dominant position. The United States has taken strong action against all of these competitors through financial, technological, and legal means. China is by no means the first or only victim of US digital hegemony and this pursuit of hegemony harms the entire international community and digital industry.

The United States intends to create an overwhelmingly dominant position for itself in cyberspace to pursue the following four goals:

First, to achieve objectively absolute security and overwhelmingly advantageous power. This is exhibited through the United States' ability to pose a deadly threat to all other actors, including states and non-state actors, at any time.

Second, to guarantee asymmetric freedom of action to the United States and its core allies as the core should have asymmetric freedom in cyberspace. Such freedom would mean that this group would be able to act without restrictions, while other actors are prevented from acting without restriction.

Third, to guarantee US companies and industries overwhelmingly leading positions in the global market, and prevent any non-US companies, even those of US allies, to challenge, pose a threat to, or overtake US companies without the US's permission.

Fourth, to have the ability to arbitrarily adjust the global division of labor according to its own needs through ideological imperialism and to achieve substantive and effective control

over the technological advancement of various actors worldwide.

The 5G Clean Path initiative is a preliminary manifestation of US digital hegemony, while the Clean Network program shows that the US has become hysterical in order to preserve its digital hegemony. The potential negative impact and damage of these programs in the mid- to long-term is clearly visible.

All state and non-state actors around the world will be at risk of retaliatory action if they become a threat to US cyber hegemony. The only way to avoid such a risk is to somehow guarantee "never" to become a competitor for the US government or US enterprise. Such hegemonic actions interfere with natural industrial development, hinder development of industries, and will eventually infringe on the digital sovereignty of other countries. Responding to the US's hegemonic actions in cyberspace and their resulting impact on 5G application and the development of other emerging technologies, the international community would need to work together. International markets must remain open to foster innovation and competition. Objective, risk-informed standards with highly transparent requirements must be established for procurement practices and guidelines. Global ICT supply chain security standards and effective confidence-building measures must be taken to mitigate the risks posed by the Clean Network program.

The Clean Network Program and US Digital Hegemony

Foreword

In June 2020, the United States State Department unveiled its Clean Network program, which consists of a series of comprehensive measures, including the establishment of a clean network list, to protect the US's sensitive corporate information and individual privacy from so-called malicious actors including China. On August 5, 2020, the Clean Network program was expanded with five new lines of effort based on the 5G Clean Path initiative to protect the US's critical telecommunications and technology infrastructure. The five new lines of effort include:

(1) Clean Carrier, to ensure that so-called untrusted Chinese carriers are not connected with the US telecommunications networks; (2) Clean Store, to remove untrusted apps from the US mobile app stores; (3) Clean Apps, to prevent so-called untrusted Chinese smartphone manufacturers from pre-installing, or otherwise making available for download, trusted apps on their apps store; (4) Clean Cloud, to prevent sensitive personal information of US citizens and corporate intellectual property from being stored and accessed on cloud-based systems accessible to foreign adversaries of the US through companies such as Baidu, Alibaba and Tencent; and (5) Clean Cable, to ensure that the undersea cables connecting the United States to the global Internet are not subverted at hyper scale by China for so-called intelligence gathering.

The Clean Network program is part of the US's basic industrial strategy, based on its other national strategies and needs. This program uses the origin of technology as its main criterion for judgment of “clean”, not objective evaluation of the technology itself. This kind of practice is highly subjective and ideologically biased and goes against industry norms, which will greatly disrupt the global industry chain. The Clean Network program is a key tool the United States will use to preserve its digital hegemony. It is a non-tariff barrier for the information industry nominally established to ensure supply chain security, whose ultimate purpose is to preserve US digital hegemony.

It should be noted that the Clean Network program is a sophisticated strategy the United States is using to crack down on the Chinese Internet industry that was created after long-term research and in-depth analysis of the industry. It is a very unusual approach taken by the US to address the challenge posed by China's Internet industry to its hegemony. The core of this strategy is based on rewriting industry rules to disrupt its current order and force related parties to re-align themselves based on ideology and other non-technical factors. This is distorting and changing the natural order of the global market.

Chinese companies such as Huawei and ZTE were not the first targets of this strategy. Japan's Toshiba, France's Alstom, Airbus, and others have been targets in the past. All of these companies fell victim to US protectionism due to their success in their respective industries, regardless of how good a relationship their home country had with the United States.

Many countries and their representative multinational companies have become natural competitors of the United States in the international market since the 1980s due to the nature of economic development and technological progress. Some have even threatened the US's dominant position. The United States has taken strong action against all of these competitors through financial, technological, and legal means. China is by no means the first or only victim of US digital hegemony and this pursuit of hegemony harms the entire international community and digital industry.

The US containment of Chinese companies, including Huawei, through the Clean Network program is a natural continuation of the US's pursuit of hegemony. Intensified strategic competition between China and the United States today has made Chinese companies targets. Other countries that have become strategic competitors will likely find themselves the targets of such actions in the future. **If this pattern of behavior fails to be effectively corrected and in fact becomes accepted as normal, the United States will presumably begin to use similar methods to obtain additional benefits in related industries where it is unsatisfied with its current benefits.**

1. US Economic Hegemony and Digital Hegemony

As the world's number one Internet power, the United States has always been committed

to seeking hegemony in cyberspace. From the US's perspective, the best way to achieve digital hegemony is work with its allies to control the Internet. It then has US high-tech companies act as Internet service providers to penetrate other countries' markets and control data on the cloud. Finally, it uses the data and intelligence it collects to form a collaborative platform to achieve digital hegemony that serves its own national interests. The United States establishes digital hegemony based on its global economic hegemony which it achieved during World War I and strengthened during World War II and has maintained to this day.

1.1 US Economic Hegemony Achieved During the Two World Wars

During the First World War, as a non-belligerent, the United States quickly accumulated massive wealth through the sale of arms. During that period, the government suspended antitrust actions, promoted scientific research, and encouraged arms sales, which indirectly laid the foundation for the meteoric rise of emerging technology industries after the war. By the end of the World War I, the United States had transformed from being a debt-laden country to the creditor of many other countries. It went from importing capital to exporting it, and went from being a debtor to a creditor.

In 1920, the United States began to enter the middle phase of industrialization. This was also a major turning point when the United States officially replaced Britain to become the new hegemon of the world. The Second World War (1939 to 1945) provided the United States with another opportunity for economic growth. The depth and scope of the impact World War II had on the growth of American wealth are unprecedented. By the end of World War II, the US's GDP was 10 times that of Britain, and its gold reserves reached 20 billion US dollars, accounting for almost two-thirds of the world's total (approximately 33 billion US dollars).[1]

It was during this period that the United States provided goods and services worth more than 50 billion US dollars to its allies under The Lend-Lease Act. Gold continued to flow into the United States, and so US gold reserves grew from 14.51 billion US dollars in 1938 to 20.08 billion US dollars in 1945, accounting for about 59% of the world's gold reserves. The international status of the US dollar was solidified due to these huge gold reserves, which

[1] Bao Shenggang, "How did the United States Rise Peacefully", Lianhe Zaobao, May 24, 2010.

allowed the United States to establish an international monetary system based on the US dollar and facilitated the expansion of the US economy worldwide.

On December 27, 1945, representatives from more than 20 countries signed the Bretton Woods Agreement and formally established the International Monetary Fund (IMF) and the World Bank (WB). This marked a new period of history in terms of international monetary systems. The Bretton Woods system was backed by gold, with the US dollar as the main international reserve currency. The US dollar was directly pegged to gold, while the currencies of various countries were pegged to the US dollar, and could be exchanged for gold with the United States at the official price of 35 US dollars an ounce. It put the US dollar at the center of the post-war international monetary system. Since then, the US dollar has become a means of payment for international settlements and the main reserve currency of various countries.

At the end of World War II, the United States began to establish international mechanisms in various fields to fill the vacuums created by the collapse of British hegemony and build its own hegemonic system. The United States has led the founding of the International Monetary Fund, the World Bank, the General Agreement on Tariffs and Trade (GATT, later known as the World Trade Organization [WTO]) and other international mechanisms to control and manage the world economy, in an effort to build its liberal international economic order.

Over the period between 1945 to 1969, the United States emerged as the leader of the capitalist camp. The emergence of a new scientific and technological revolution in the United States, marked by the development of atomic technologies, aerospace technologies, and computing technologies, has made the US economy highly modernized. In addition, modern American corporate organizations, and national and international monopolies have all enjoyed new developments, resulting in the rise of many multinationals. All of these made the United States a highly modernized superpower and set the stage for the post-industrial society and information society. The third industrial revolution represented by nuclear energy, computing, and aerospace technologies promoted the shift in global supply chains that allowed the United States to position itself at their core.

1.2 US Economic Hegemony as the Foundation of Digital Hegemony

The US's economic hegemony set the stage for its digital hegemony. The US has had clear

and unique advantages when it came to the evolution of the Internet. It was not only the birth place of Internet technologies, but it was also the largest controller of Internet root name servers. The United States controls the world by controlling the network, thereby consolidating its position as a hegemon. In the third technological revolution following World War II, the United States created a monopoly for itself in resource allocation, technical standards setting, and content generation. Its dominance over the distribution of Internet resources and key links in the industrial chain created the foundation of US digital hegemony.[2]

At present, every key link in the global Internet industrial chain, including operating systems, chip design, and software, is dominated by the United States. This dominance has given the US an absolute advantage in cyberspace, allowing it to run unbridled eavesdropping and monitoring programs around the world, further shoring up its digital hegemony. The United States has also set global Internet technology standards to gain control of the telecommunications industry. The United States finally also legitimatized its hegemonic policies by formulating international rules for cyberspace. Both the Obama administration and the Trump administration have continuously taken steps to tie the Internet to national security by introducing a series of cyberspace strategies that would consolidate its dominant position in cyberspace and preserve its cyber hegemony. The Clean Network program is in line with these previous national strategies on cyberspace. Like its predecessors, it reflects the US's overall strategy for cyber hegemony in the digital industry and is intended to preserve the US's global digital hegemony in the new era.

After the Cold War, the United States consolidated its hegemony in the political and security fields through superior military capabilities and preserved its economic hegemony with financial, technological and legal systems as globalization sped up.

[2] Du Yanyun, "Analysis of the Paths towards US Cyber Hegemony", Pacific Journal, Vol.24, No.2, 2016.

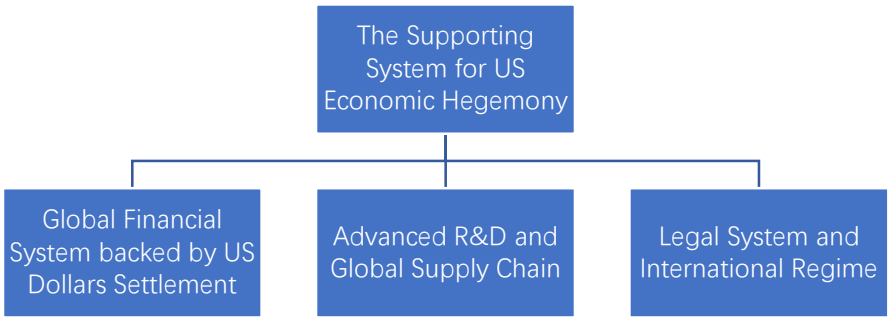

Figure 1: The US Economic Hegemony System

2. The US's Tradition of Preserving Economic Hegemony by Attacking the Competition

Due to the nature of economic development and technological progress, there has always been other countries, including US allies (such as Japan and other major countries in Western Europe in the 1980s and 1990s), and representative multinational companies from those countries that would compete with and even threaten the dominance of the United States and US companies in the international market.

The United States has consistently suppressed these competitors by taking severe financial, technological, and legal measures against them. Financially, the US would take advantage of the dominant position of the dollar to impose unique financial sanctions on companies or by denying them access to dollar settlement for transactions. Technologically, the US would introduce bans on export and export control measures or cut or reorganize the supply chains those enterprises relied on. Legally, the US initially relied on the international multilateral system provided by the WTO, however, as other countries continue to grow in strength and gained a deeper understanding of WTO laws and procedures, the United States began to paint the international system as inefficient.

As the United States gradually lost effective *de facto* control over the international multilateralism platform and other countries grew in power, the US began to return to bilateral and unilateral frameworks, frequently use domestic legal procedures (including Section 301 investigations), and use different policy toolsets (such as long-arm jurisdiction and the Entity List) to weaponize compliance issues and politicize trade and technology. Designating the

above issues arbitrarily as national security issues has since become customary and so more subjective and arbitrary approaches to preserving US hegemony have been adopted.

2.1 Sanctions and Attacks Using the US Dollar Payment System as a Core Tool for Financial Hegemony

Unilateral financial sanction is one of the most powerful weapons the United States has in its arsenal. The US dollar's critical role in global commodity and capital transactions made observance of such sanctions directly compulsory. The SWIFT-based US dollar cross-border clearing system and cross-border financial infrastructure specifically realizes this. Founded in 1937, SWIFT is now a global financial infrastructure that spans more than 200 countries and territories, and provides more than 11,000 institutions around the world with secure messaging services and interface software. As an important component of the US dollar-led international settlement system, it is impossible for any individual, corporate organization, or country that does business extensively around the world to bypass. The SWIFT system also allows the United States to gather financial data that can be used to accurately identify sanction targets and formulate sanction measures. This dynamic monitoring can also be used to ensure the effectiveness of economic sanctions. The use of the US dollar payment system to sanction and attack companies is most common when US economic interests are damaged or its market position is threatened. The US sanctions on the Nord Stream 2 project is a typical example of this kind of attack.

Nord Stream 2 is an offshore natural gas pipelines between Russia and the European Union. The goal of the line is to supply 55 billion cubic meters of natural gas to EU countries each year through the Baltic Sea and Germany. However, the project faced opposition from the United States. In January 2019, Richard Grenell, the US Ambassador to Berlin, said that Nord Stream 2 would threaten Ukraine's security and political importance and increase the threat of Russia intervention in conflicts in Ukraine. In addition, the project would make Europe dependent on Russia's energy supply. He warned that companies involved in the project would suffer damage to their corporate reputation and incur the potential risk of sanctions.

To address these concerns, Russia, the European Union, and Ukraine held negotiations on natural gas issues at the European Union headquarters in Brussels and came to their own

agreement on December 19, 2019. Despite this, US President Donald Trump signed and passed the National Defense Authorization Act for Fiscal Year 2020 the next day, imposing sanctions on the companies involved in the construction of Nord Stream 2. Germany strongly opposed this move.

The geopolitical and economic motivations behind the US's actions are clear. The United States wanted to export liquefied natural gas (LNG) to Europe. The successful completion of the Nord Stream 2 project would allow Russia to replace the United States in Europe's LNG market, which will not only damage United States economic interests, but also reduce its say over European affairs.

2.2 Extreme Pressure on Companies Through Export Controls and Bans to Paralyze or Even Cut Off the Supply Chain

The second common method for the United States to preserve its economic hegemony is introducing export controls and bans for the purpose of putting extreme pressures on targeted companies via paralyzing or even cutting off the supply chain. One way is by exercising control over the export of military products, dual-use products, and technology according to domestic export control laws such as the Export Administration Act (EAA), the Arms Export Control Act (AECA), and the International Emergencies Economic Power Act (IEEPA). Another way is by uniting its allies and major Western countries via the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (the Wassenaar Agreement) to control the export of military products, dual-use products, and high-tech products to China and elsewhere.

During the Cold War between the United States and the Soviet Union after World War II, in order to prevent the Soviet camp from developing high-end weapons, with proposal from the United States, 17 countries including the United States, Britain, Japan, France, Australia established the Coordinating Committee for Multilateral Export Controls (CoCom) in Paris in November 1949, putting restrictions on the exports of strategic materials and high-end technologies to socialist countries by member states. After the collapse of the Soviet Union, CoCom was formally dissolved on April 1, 1994. Two years later, the Wassenaar Agreement led by the United States was signed in Vienna, Austria, inheriting the embargo policy of CoCom.

The agreement became an important means for the United States to contain and oppress the development of high-tech industries in foreign countries. This second method is often used when companies in other countries threaten the technological leadership of the United States. Well-known cases are Japan's Toshiba incident and Europe's Airbus case (The ECHELON Affair).

In the 1980s, the United States and Japan competed fiercely to dominate high-tech industries. In 1987, Toshiba Machinery, a subsidiary of the Toshiba Group, was found to have secretly exported computerized propeller milling machines to the Soviet Union which were used to make submarines quieter. Subsequently, the US launched investigations into Toshiba Machinery and economic sanctions against Japan as well.

As shown in Table 1, the Semiconductor Industry Association (SIA) filed a lawsuit in 1985 regarding dumping by Japanese semiconductor companies with the Office of the United States Trade Representative (USTR). As a result, the United States initiated a Section 301 investigation into Japanese electronic products. In 1986, the US and Japan signed the US-Japan Semiconductor Agreement, which included ending Japan's dumping practices, reducing Japanese semiconductor exports to the US, and encouraging Japan to increase the market share of American semiconductor products to 20%. The first five-year US-Japan Semiconductor Agreement expired in 1991. The two countries signed a second five-year agreement on semiconductors, and the market share of American semiconductor products in Japan continuously increased. US semiconductor companies gradually recovered their competitiveness and surpassed Japanese companies in global market share by the mid-1990s.

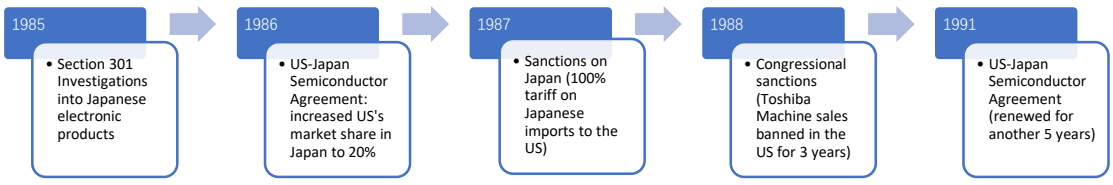

Table 1: US Investigations into and Sanctions on Japan after the Toshiba Incident

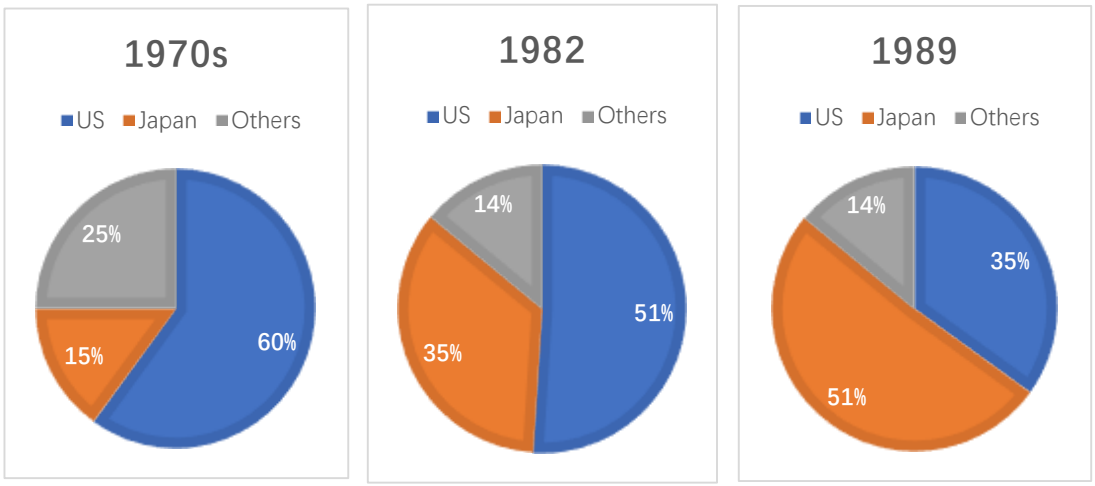

Figure 2: Global Market Share of American and Japanese Semiconductor Products[3]

The "Toshiba Incident" appeared to be a trade friction between the US and Japan regarding the violation of export controls established by the CoCom. However, Japan's Toshiba Machinery was not the only transaction party involved, Norway's state-owned military company Kongsberg was too. These two companies worked together to complete the computerized propeller milling machines exported to the Soviet Union. Their cooperation made this export control violation a multinational trade issue. However, the US targeted Toshiba Machinery, which indicates that the US was not merely hoping to maintain the CoCom embargo, but also to protect its leading position in high-tech.

As a major strategic industry, the semiconductor industry is an important indicator of a country's technological leadership. As shown in Figure 2, the US semiconductor industry had complete dominance globally with 60% of the market share in the 1970s. At that time, Japan's semiconductor industry was far behind the US's and its global market share was about 15%. In 1980s, Japan's semiconductor industry developed rapidly. By 1982, it had occupied 35% of the global market share, threatening the dominance of the US in the semiconductor industry. A report by the US Department of Commerce in 1983 pointed out that in the five high-tech fields, the US only maintained a leading position in aircraft manufacturing and aerospace technology, while lagging behind Japan in semiconductors, optical fiber, and intelligent machinery.[4]

The US's economic hegemony since World War II needed to be supported by its leading

[3] Source: "The U.S.-Japan Semiconductor Agreement: Keeping Up the Managed Trade Agenda", *The Heritage Foundation*, January 24,1991, https://www.heritage.org/asia/report/the-us-japan-semiconductor-agreement-keeping-the-managedtrade-agenda.

[4] Hou Wenfu. 2000. "Toshiba Incident and its Impacts", *Riben xuekan [Japanese Studies]* 2000(1), p. 46.

position in high tech. The rapid development of the Japanese semiconductor industry in the 1980s challenged American leadership in advanced technologies. As a consequence, Japan was investigated and sanctioned by the US and was forced to sign a semiconductor agreement to not only reduce imported semiconductor products by the US, but also to maintain the market share of American semiconductor companies in Japan. These actions reflect the US's support of its own economic hegemony. Especially when faced with the decline of its own technological superiority, the US imposed tariffs and semiconductor agreements to restrict the export of Japanese electronics and the development of Japan's semiconductor industry. The timeline for the US to launch trade investigations and economic sanctions against Japan regarding the Toshiba incident coincides with Japan's semiconductor industry taking off. This indicates the true motives of the US concerning this situation.

It needs to be noted that the way the US oppressed the Japanese semiconductor industry was by destroying Japan's manufacturing capacity of finished semiconductor products (i.e., memory sticks at that time), and then forcing Japan to move up the accessory manufacturing supply chain to produce photoresist and the like. It seems that this kind of movement was in step with technological progress. Nevertheless, at a national level, it meant that Japan and the Japanese companies involved in the global industrial system were marginalized and lost their autonomy. Only when cooperating with American strategies, such as blockading the industrial chain and the exclusion strategy, can Japan play a substantive role. Otherwise, Japan's movement to the upper end of the accessory manufacturing industry can only exert limited influence on the restricted disputes between Japan and South Korea.

A more extreme example is the non-commercial model of the alliance between American companies and the government in commercial activities. Between 1994 and 1995, Airbus lost to Boeing in a bid for an aircraft contract with Saudi Arabia worth 6 billion US dollars. Suspecting unfair competition, Airbus filed a complaint with the European Union, and the EU set up a temporary committee to investigate into the issue. It turned out that Boeing provided a global electronic surveillance system called "Echelon" for the Five Eyes alliance. The US National Security Agency (NSA) used this surveillance system's telecommunication satellite interception function to obtain all faxes and telephone calls between Airbus and the Saudi government as well as airlines from a commercial communications satellite. By analyzing the

content, the US believed that Airbus agents bribed Saudi officials. The US government provided numerous trade secrets to Boeing, which contributed to two American companies, namely, Boeing and McDonnell Douglas winning Saudi Arabia's aircraft contract.

What's interesting is that in the case of US surveillance of trade secrets (i.e., the European Airbus case), all the victimized companies or individuals were seen as "criminals" by the US government. They were accused of commercial bribery, illegal transfers, patent theft, etc. Moreover, the report of the Temporary Committee found that there are many similar cases in which the US has carried out commercial surveillance to give American companies an advantage in competition. There are more than 20 cases that have been made public, covering many famous enterprises from Japan, France, Germany, and Israel among others. But what is even more shocking is that after the incident was revealed, R. James Woolsey, the former director of US Central Intelligence Agency, published a signed article in the *Wall Street Journal* entitled "Why We Spy on Our Allies". **He argued that this kind of surveillance is a necessary condition for American companies to compete on a level playing field.**

In short, the European Airbus case reflects the double standards and the hegemonic logic of the US. That is, the US has the most advanced technology, so it is reasonable to win in various commercial bids; whereas Europe falls behind the US with respect to technology, costs, quality, market share, etc. If a European company beats American companies, then either that European country or that company must have resorted to illegal measures such as bribery. In other words, only when the United States has a complete technological, economic, and social advantage can the world be regarded as being truly "fair and reasonable". This logic remains the same in the current US economic pressure on China.

2.3 Using Domestic Legal Procedures, Long-arm Jurisdiction, and the Entity List to Contain Companies

Globalization has led to deep interdependence among countries around the world, but there are asymmetries in this dependence. In international relations, these asymmetries bring power to the dominant party in complex interdependence. To put it another way, one country can use

these asymmetries to force the targeted countries to change policy behaviors and concede.[5] As the world's only superpower, the third method that the US often adopts to preserve its economic hegemony is to use its domestic legal procedures, long-arm jurisdiction, and the Entity List to contain companies. Since the 1980s, the US has targeted Japanese and European companies.

The rapid development of the Japanese computer industry in the 1970s threatened the original dominance of the US. In 1982, an undercover FBI agent falsely claimed to possess the latest IBM computer technology and used an entrapment scheme to induce Hitachi and Mitsubishi Electric employees to purchase the technology. After the two companies got the relevant blueprints, the FBI quickly arrested 6 "commercial spies" and issued warrants for 12 Japanese employees. Hitachi and Mitsubishi Electric had to reach an agreement with IBM on the payment for the use of its technology, and in 1983 alone, Hitachi paid about 10 billion yen.

For the past ten years, under the guise of an overseas anti-corruption and violation of sanction, the US Department of Justice sued the executives of European high-tech companies and imposed hefty fines, and thus successfully oppressed and destroyed many large multinational companies in Europe.

As the crown jewel of French industry, Alstom had ranked first globally in hydropower equipment, nuclear power (conventional islands), environmental control systems, super high-speed trains, and high-speed trains. It ranked second in urban transportation, regional trains, infrastructure equipment, and all other related services. Additionally, Alstom also performed well in energy-related fields. It provided equipment that accounts for 15% of the world's installed electricity capacity. Moreover, it has ranked second globally in transportation as well as electric power transmission and distribution.

Alstom had been investigated by the US Department of Justice for more than three years by 2013, but at that time Alstom CEO Patrick Kron decided not to cooperate with the US authorities. For the purpose of weakening Alstom and imposing sanctions on it, the FBI arrested the ex-Alstom executive Frédéric Pierucci at a US airport in 2013, and he was prosecuted and imprisoned. The US Department of Justice accused Pierucci of commercial bribery and

[5] Xu Feibiao. 2019. "Meichangbiguanxia de qiyuan kuozhang ji yingdui [The Origin, Expansion and Response of the US Long-arm Jurisdiction]" *Zhongguo Waihui [Journal of China Foreign Exchange]*, 2019(14): 32-35.

imposed a 772 million US dollar fin[6]e on Alstom. After seeing Pierucci being arrested, Alstom panicked, and its executives began to cooperate fully with the US Department of Justice. In order to save himself, Alstom's CEO negotiated in secret with General Electric (GE) and sold three-quarters of the company's business, including power, to GE. Despite the intervention of the European Union, GE still successfully acquired Alstom's business and obtained the right to maintain all French nuclear power plants, which provides 75% of France's electricity. This acquisition has also changed the competitive structure of the global energy equipment industry. General Electric from the US, Siemens from Germany, and ABB from Sweden have begun to dominate the global energy equipment market.

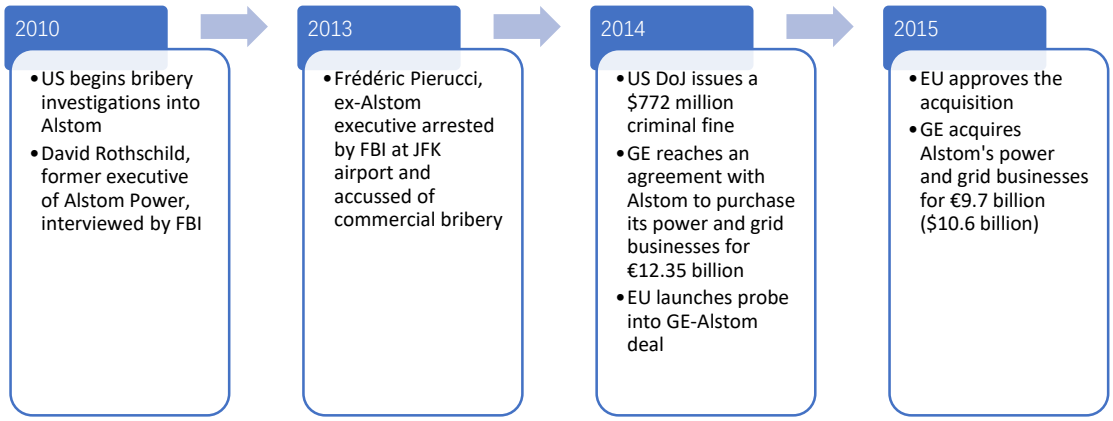

Table 2: Timeline of Alstom Bribery Case

With regard to investigations involving the US Foreign Corrupt Practices Act (FCPA), 30% (474) of the cases from 1977 to 2014 were directed at non-US companies, which paid 67% of the total fines. Of the 26 companies that were fined over $100 million, only 5 were US companies, and of the other 21 non-US companies, 14 were European. As shown in Figure 3, so far, none of the top ten largest US monetary sanctions were imposed on American companies.

[6] US Department of Justice, "Alstom Pleads Guilty and Agrees to Pay $772 Million Criminal Penalty to Resolve Foreign Bribery Charges", December 22, 2014, https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery.

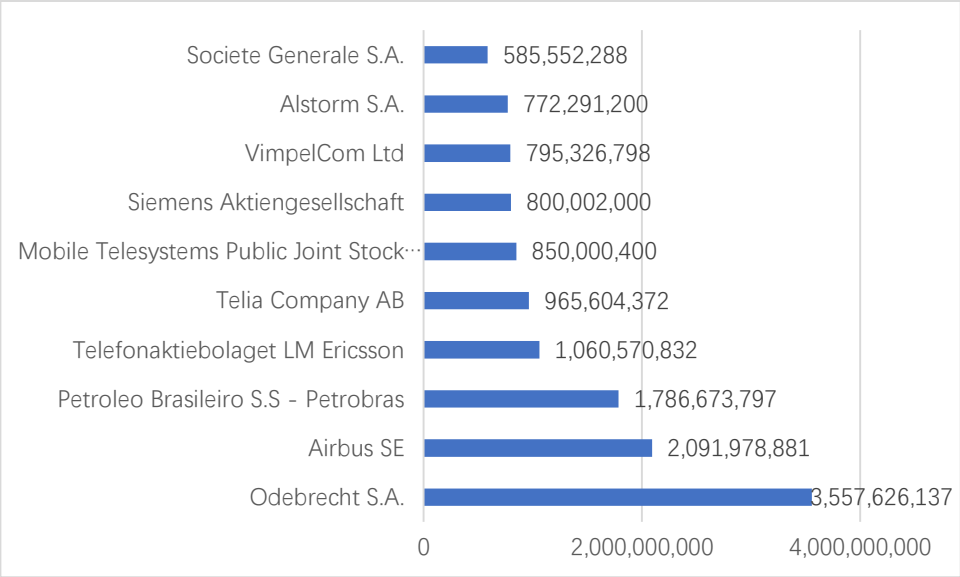

Figure 3: Largest US Monetary Sanctions by Entity Group (FCPA, in USD)[7]

This shows that any enterprise or even nation, including US allies, that challenges the US's economic hegemony will be severely oppressed and sanctioned by the US. In recent years, with the rise of developing countries and emerging market economies, there are an increasing number of cases where the US has used domestic legal procedures, long-arm jurisdiction, and its Entity List to oppress enterprises from other countries. The Special 301 report is published by the Office of the USTR annually on the protection of intellectual property rights in countries around the world, and since 1989, the United States has issued nearly 30 of these reports.

The number of countries covered in the Special 301 report has increased from year to year, from 25 in 1989 to 70 in 1998. The targeted countries have also shifted from mainly developed countries and a few developing countries, now onto developing countries and emerging economies. Moreover, the issues involved in the Special 301 report have gradually exceeded the scope of intellectual property rights, covering anti-corruption, environment, and public health.

With the release of the Special 301 reports, the US unilaterally sets standards, unilaterally issues reports, unilaterally gives interpretations, unilaterally launches investigations, and unilaterally imposes sanctions on targeted countries. These exert significant pressure on

[7] Source: Largest U.S. Monetary Sanctions by Entity Group, Stanford Law School Foreign Corrupt Practice Act Clearinghouse, http://fcpa.stanford.edu/statistics-top-ten.html.

targeted countries and force them to give into the American hegemony. The US has thereby preserved its superiority in the field of intellectual property, trade, and investment. In addition, the Special 301 reports are also important bargaining chips for the US when negotiating with other countries. By dominating the conversation and taking the moral high ground, the US forces other countries to make concessions in related fields.

3. The US Insists on Using Traditional Financial, Technological, and Legal Means to Maintain Digital Hegemony

The US is still in a dominant position moving from establishing a traditional economic hegemony to digital one, although the US dollar payment system has been impacted. The United States still uses financial tools to suppress competitive companies in the digital sector, and also prevents the digital payment industry from further impacting the US dollar payment system. Despite the fact emerging countries continue to advance and certain countries have gradually upgraded their industries to move up the value chain, the United States and its technology have completely penetrated and integrated itself into every part of the global supply chain, making it possible for them to adopt outright bans to suppress certain companies.

Lastly, laws and international systems are currently lacking in international rules on the digital economy. Major powers have frequent disputes about cross-border data flow and trading technologies. The WTO has all but failed, and the United States frequently employs domestic laws, administrative orders, and sanctions against competitors on the grounds of national security, and attempts to shape a global digital industry and ecosystem dominated by the United States.

3.1 Suppressing the Development of Foreign Companies by Weaponizing Compliance

As the first Chinese social product to truly win over foreign users, TikTok has reached 500 million monthly active users worldwide since 2018, making it the most downloaded app on App Store. However, since 2019, the United States has hyped up TikTok's security threats, getting the app into hot water on a global scale. The United States first accused TikTok's parent company ByteDance of sharing data with the Chinese government and then claimed that TikTok suppressed speech through content censorship. In addition, the United States has been seeking

to weaponize compliance issues in response to the rise of TikTok on a global scale. **Weaponization here is to start from the technical level by reviewing TikTok on the issues of so-called personal privacy information collection, cross-border data transmission, content review, relations with the Chinese government, and other seemingly technical and procedural details. After discovering that TikTok resolved these technical issues in terms of form, procedure, and operation one by one, it directly used "pockets" of "suspected threats to national security"** to apply extreme pressure in a way that did not allow TikTok to respond and defend.

First, TikTok was reviewed for security, and then a download ban against TikTok was issued by federal agencies. Recently, the United States directly requested American capital to make a compulsory acquisition of TikTok through an administrative order. This approach in the United States has disrupted fair competition, allowing traditional American social media giants to obtain market share outside the usual way, and this will also raise questions about the status of the US market economy.

3.2 Sophisticated Crackdown on Companies Through Technology Control, Export Bans, and Other Measures

The sophisticated crackdown on companies through technology control, export bans, and other methods is exemplified by the cases of DJI and Huawei. DJI Innovations, the world's largest civilian drone manufacturer, is a Chinese tech company that mainly produces and develops unmanned civilian aerial vehicles and aerial photography systems. The company's drones have won the support of aerial photographers and photography enthusiasts all over the world, occupying 70% of the global market. However, since 2017, the US government has looked for various reasons to suppress its drone products. US customs officials said in a report that officials have "moderate confidence" that DJI's commercial drones and software are "providing US critical infrastructure and law enforcement data to the Chinese government".

On May 20, 2019, the US Department of Homeland Security targeted DJI on the grounds of user information security issues. In October, legislation was introduced to ban all federal agencies from using drones manufactured or assembled in China, and in November, the US Department of the Interior announced that it would ground all UAVs in its fleet that were made

in China or contained components made in China. Due to the market positioning and quality of DJI UAVs, no UAV manufacturer could completely replace it. Therefore, the US government has repeatedly sought technological control measures to curb DJI's development. Although DJI has made many changes, it still faces pressure from the United States. The US may still surpass the current technological control measures and resort to administrative measures to crack down on DJI. For example, it could put DJI on the Entity List to prohibit direct dealings with American companies.

In August 2018, Trump signed the US National Defense Authorization Act for Fiscal Year 2019. Article 889 of the bill prohibits all US government agencies from purchasing equipment and services from Huawei. The United States continued to escalate its suppression of Huawei by putting it on the Department of Commerce's Entity List, which prohibited US companies from selling chips to Huawei. On May 15, 2020, the US Department of Commerce announced that it would protect national security by restricting Huawei's ability to use US technology and software to design and manufacture its semiconductors abroad. After the export rules were changed, foreign companies using US chip manufacturing equipment will be required to obtain US licenses before supplying certain chips to affiliates such as Huawei or HiSilicon. On August 17, 2020, the United States further tightened restrictions on Huawei by requiring special permission to sell chips made using US technology to Huawei and by plugging potential loopholes present in the May sanctions. These loopholes allowed Huawei to obtain related technologies through third parties. The United States is trying to not only stop Huawei's technological development by cutting off supplies to Huawei, but also by preventing other countries from purchasing Huawei's 5G equipment.

The US abuses its national power to block and suppress Huawei without a bottom line, which is characteristically hegemonic. From an industrial perspective, related reports by the Boston Consulting Group show that the Sino-US trade tensions may cause the two countries' semiconductor industries to decouple, and US semiconductor revenues will fall by 37%, which is about 83 billion US dollars if based on the industry's revenues for 2018. About three-quarters of the decline in revenue will come from Chinese customers having to replace American semiconductors due to the US ban on technology exports. It can be seen that this move violates the objective laws of the industry and will cause severe harm to global industrial development.

3.3 Taking Advantage of Its Ability to Reformulate International Rules to Squeeze the Legitimate Interests of Allies

On December 10, 2019, the United States, Mexico, and Canada signed the new US-Mexico-Canada Agreement (USMCA) that went into effect on July 1, 2020, replacing the 25-year-old North American Free Trade Agreement (NAFTA). Since 2017, the US government has repeatedly criticized the agreement for draining manufacturing jobs from the US, and had asked for renegotiations by threatening to withdraw from the treaty. Therefore, the new USMCA has become regarded as one of the main achievements of President Trump during his administration, and the US government has even touted it as "the highest standard trade agreement of the 21st century". However, many provisions in the agreement once again reflect the digital hegemony of the United States. It does so by not only expanding the scope of cross-border data flow by prohibiting the localization of personal data in a mandatory and binding way, but also by extending this restriction to the financial sector, which can help US financial regulators obtain Mexican and Canadian financial data.

Google, Facebook, Apple, and Amazon operate in many countries and garner massive revenue, but they choose low-tax areas to register their headquarters to "legally" evade taxation. This exposes traditional industries and small and medium-sized tech companies to unfair competition in the country where users are located. Governments suffered loss, which upset EU member states such as France and Italy. In March 2018, the European Commission announced a legislative proposal that any EU member state can tax the profits generated by Internet activity occurring within its borders. Realizing fair tax payment by Internet companies is a global issue, and no single country can solve it on its own. After France proposed a digital tax, the United States immediately announced that it would impose tariffs on France as a countermeasure. In June 2020, the United States withdrew from negotiations on the digital taxation of multinational tech companies under the framework of the Organization for Economic Cooperation and Development, this time on the grounds of the pandemic. The above cases all reflect that the United States relies on its leverage in international negotiations and uses loopholes in international rules to gain an unfair advantage.

4. Clean Network Program as a Key Attempt by the United States to Achieve Digital Hegemony

On April 29, 2020, US Secretary of State Mike Pompeo announced that the State Department would begin requiring a 5G Clean Path for all 5G network traffic entering and leaving US diplomatic facilities. This prevents all IT suppliers deemed "unreliable" (including ZTE and Huawei) from accessing 5G networks in countries worldwide in any way, including transmission, control, computing, and storage. The initiative is part of the Clean Network program, which was launched in June 2020. On August 5, 2020, the United States updated the Clean Network program to include five new lines of effort to protect the critical telecommunications and technology infrastructure of the United States. At this point, the Clean Network program essentially covers all of the ecological closed-loop supply chain, in an effort to prevent Chinese Internet companies from challenging the US-dominated Internet world, and ultimately preserve the digital hegemony of the United States. **This marks the first time that the United States, with no overwhelming advantage in a real industrial sense, has made a serious attempt to seek cyber hegemony mainly through non-industrial and non-technological approaches.**

4.1 The Clean Network Program is Essentially a Non-tariff Barrier Established on the Grounds of Supply Chain Security

As China takes the lead in the development of advanced network information technology and the digital economy, represented by 5G, the notions of the so-called "red tech threat" and "digital orientalism" are becoming prevalent in the United States. This is essentially a narrative that has grown from a binary opposition perspective that any Chinese information technology will be used for surveillance and national security purposes, and that any Chinese digital economy applications will have privacy issues.

Furthermore, this thought process concludes that China's achievements in technological research and development, and economic development must be founded on dishonest practices, including cyber-theft and violation of market economy rules. This type of rhetoric could rally

the US and the entire Western world against the ancient mysterious countries of the East by stoking fear and arousing nationalist sentiment. In addition, it could serve to absolve major developed Western countries of the responsibility for technical and economic decline, and reunite the people of the West to recognize their own civilizations and systems.

Through the Clean Network program, it is claimed that all aspects of China's information technology products and services will be excluded from telecommunications services, APP stores, applications, cloud services, cables, and 5G. The program is highly subjective, and its definition of "clean" is rife with ideological bias that anything that is not related to a Chinese supplier is inherently "clean", while anything that the US considers unacceptable is "unclean". However, the US does not define "clean" by objectively judging the technology itself, but primarily according to the origin of the technology. Therefore, the Clean Network program can be seen as a sophisticated US crackdown on China's Internet industry from a full supply chain perspective. This essentially makes it a non-tariff barrier established on the grounds of supply chain security.

4.2 The Clean Network Program is a Policy Toolkit for the United States to Achieve Digital Hegemony

In June 2020, the United States State Department unveiled its Clean Network program, which consists of a series of comprehensive measures, including the establishment of a clean network list, to protect the US's sensitive corporate information and individual privacy from so-called malicious actors including China.

As shown in figure 4, on August 5, 2020, the Clean Network program was expanded with five new lines of effort based on the 5G Clean Path initiative to protect the US's critical telecommunications and technology infrastructure. The five new lines of effort include: (1) Clean Carrier, to ensure that so-called untrusted Chinese carriers are not connected with the US telecommunications networks; (2) Clean Store, to remove untrusted apps from the US mobile app stores; (3) Clean Apps, to prevent so-called untrusted Chinese smartphone manufacturers from pre-installing, or otherwise making available for download, trusted apps on their apps store; (4) Clean Cloud, to prevent sensitive personal information of US citizens and corporate intellectual property from being stored and accessed on cloud-based systems accessible to

foreign adversaries of the US through companies such as Baidu, Alibaba and Tencent; and (5) Clean Cable, to ensure that the undersea cables connecting the United States to the global Internet are not subverted at hyper scale by China for so-called intelligence gathering.

The Clean Network program was designed to cover the entire telecommunications supply chain and ecosystem. It represents a sophisticated strategy from the United States, based on long-term research and in-depth analysis of its target, which they intend to use to crack down on China's Internet industry. The program can be viewed as a toolkit for achieving digital hegemony. The United States has used its national power to unilaterally encircle Chinese companies so that Chinese Internet companies cannot challenge the US-dominated Internet world, with the ultimate goal of preserving US digital hegemony.

Figure 4: The Clean Network Program

4.3 The Clean Network Program Will Harm Other Countries' Digital Sovereignty and Hold Back the Development of the Industry

As the Clean Network program is implemented to realize US digital hegemony, it will undermine other countries' digital sovereignty. First, every country has the freedom to choose its own trusted carriers and services, a freedom that the Clean Network program would deny to the countries concerned. Second, the US has brought telecoms carriers, mobile applications, mobile APP stores, cloud services, cables, and 5G providers under the control of its Clean Network program. This level of control will infringe on the autonomy of other countries regarding the operation and regulation of the Internet. Finally, as data is an important national asset, countries may want to tighten up regulations regarding data localization and local

operations. However, the long-arm jurisdiction over data in the US, through the Cloud Act, would severely undermine the data autonomy of the countries concerned.

It should be noted that this attempt by the United States to seek cyber hegemony has drawn backlash from communities that traditionally supported and endorsed asymmetric US governance of global cyberspace, in addition to scholars with classically liberal views:

As Milton Muller, professor at the Georgia Institute of Technology and founder of the Internet Governance Project, put it, "The Clean Network program is an attempt to fragment the Internet and the global information society along US and Chinese lines, and shut China out of the information economy. This could backfire on Silicon Valley giants which dominate the online world outside China because there are lots of nationalistic governments around the world which could make the same claims about Apple and Google and Facebook and Twitter that they are sucking up data. Mr. Trump's actions are based on nebulous security concerns and a misguided notion of countering China's rising power. The idea that the US can stop Chinese development by cutting them off is stupid; it's not going to happen."[8] Daniel Castro, vice president of the Information Technology and Innovation Foundation, also said, "The United States should be careful about arguing that there is an inherent national security risk of using technologies from foreign companies. If other countries apply that same logic, US tech companies will be locked out of many foreign markets, posing a serious risk of Internet fragmentation."[9]

5. Recommendations for Resolving the Risks of the Clean Network Program

The United States has built a captive relational order in cyberspace which strives to ensure that the US gains overwhelming superiority. This is specifically embodied by four aspects. First, the United States must be objectively safe. Second, the US requires asymmetric freedom of operation in global cyberspace. Third, American companies must hold an overwhelmingly leading position across the entire industry, and potential rivals of US companies cannot occupy this position, even those from allied countries. Fourth, the US strategy does not account for the

[8] Rob Lever, "Trump moves on China apps may create new internet 'firewall'", Tech Xplore, August 7, 2020, https://techxplore.com/news/2020-08-trump-china-apps-internet-firewall.html

[9] Ibid.

trend of globalization and the reasonable demand for specific and endogenous industrial division of labor. Instead, it displays strong ideological and subjective attributes. Such a dominant structure would seriously disrupt the global market and seriously damage the industry as a whole in all countries worldwide. The Clean Network program is essentially a non-tariff barrier that uses the maintenance of supply chain security as an excuse. It violates the objective laws of technology and business, damages the digital sovereignty of other countries, and hinders the development of the industry. Therefore, the international community should collaborate to create a fair and competitive environment for the industry, formulate objective and reasonable standards, and take effective measures to build trust in order to resolve the risks brought about by the Clean Network program.

5.1 Maintain an Open Market, Create a Level Playing Field for ICT Suppliers, and Avoid the Creation of Trade Barriers

In response to the US adding Chinese companies to the Entity List in the name of national security, on May 31, 2019, China's Ministry of Commerce announced that it would establish an Unreliable Entity List. This was intended to counteract the Entity List and targeted American companies and associations. As the second largest economy in the world, China has extensive economic ties with the rest of the world, particularly the European Union.

Since the establishment of formal relations between China and the European Economic Community in May 1975, China and the EU have established cooperative partnerships, comprehensive partnerships, and comprehensive strategic partnerships. The EU has now been China's largest trading partner for 16 years, and both sides have broad and extensive common interests. Therefore, the EU should look to maintain an open market, create a level playing field for Chinese ICT suppliers, and avoid creating non-tariff barriers under the pretext of national security. This is the only way the EU will ensure mutually beneficial economic interactions with China, and avoid Chinese countermeasures to discriminatory treatment of Chinese companies.

5.2 Develop Procurement Practices and Guidelines Based on International Standards and Approaches

High-level, global ICT certification and testing programs that have international influence can enhance the security and credibility of ICT. By establishing a compliance program run by global organizations (whether existing or new organizations), we can greatly reduce costs related to technical security tests and applications. This will provide compliance standards and best practices that benefit customers and stakeholders. The international community should collaborate to develop international standards based on technological neutrality and non-discrimination. We should establish risk-informed procurement practices and guidelines that have objective standards and transparent principles. At the same time, every country should oppose discriminatory, self-centered standards that are based on subjective judgments. This will allow countries worldwide to maximize their national interests and obtain global resources in the most cost-effective way when developing the information industry represented by 5G.

5.3 Establish Security Standards for the Global ICT Supply Chain and Take Effective Measures to Build Confidence

The European Union Agency for Cybersecurity (ENISA) released the report *Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward* in 2012, which it updated in 2015. In addition to providing lessons for participants in the ICT supply chain, the report recommends the establishment of public-private partnerships in order to build an international assessment framework and evaluate ICT supply chain risk management. Meanwhile, other states, including China and Russia, put forward the *International Code of Conduct for Information Security* to the United Nations, which outlines specific initiatives to ensure the security of the ICT supply chain:

> *To endeavor to ensure the supply chain security of ICT products and services, prevent other states from using their resources, critical infrastructures, core technologies and other advantages, to undermine the right of the countries, which accepted this Code of Conduct, to independent control of ICTs, or to threaten other countries' political, economic and social security.*[10]

[10] International Code of Conduct for Information Security. Ministry of Foreign Affairs of the People's Republic of China. Dec.9.2011 https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t858323.shtml (log in

These are all good practices that help build confidence between countries and between enterprises and customers, and promote the sound development of the entire industry.

Sep.1.2020 20:30)

Appendix 1: Cases Published in the REPORT on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System).

Case	Who	When	What	How	Aim	Consequences
Air France	DGSE	Until 1994	Conversations between travelling businessmen	Bugs were discovered in the first class cabins of Air France aircraft – public apology by the company	Obtaining information	Not stated
Airbus	NSA	1994	Information on an aircraft order concluded between Airbus and Saudi Arabian Airlines	Interception of faxes and phone calls between the negotiating parties	Forwarding information to Airbus' US competitors, Boeing and McDonnell-Douglas	American companies won the contract (US$6 bn)
Airbus	NSA	1994	Contract with Saudi Arabia worth US$6 bn	Interception of faxes and phone calls, routed via telecommunications satellites, between Airbus and Saudi Arabian Airlines/the Saudi Government	Uncovering of bribes	McDonnel-Douglas, Airbus' American competitor, won the contract
BASF	Marketing manager	Not stated	Description of the process for producing a raw material for skin creams by BASF (cosmetics division)	Not stated	Not stated	None. The attempt was discovered

Federal German Ministry of Economic Affairs	CIA	1997	Information concerning high-tech products held by the Federal Ministry for Economic Affairs	Use of an agent	Obtaining information	Agent unmasked and expelled from the country
Federal German Ministry of Economic Affairs	CIA	1997	Background information of the Mykonos trial in Berlin, Hermes loans concerning exports to Iran, and establishing German firms supplying high-tech products to Iran	A CIA agent disguised as a US ambassador holds friendly conversations with the Head of the Department in the Federal Ministry for Economic Affairs responsible for the Arab region (particular responsibility: Iran)	Obtaining information	Civil servant contacts the German security authorities who inform the Americans that the CIA operation is unwelcome. CIA agent then 'withdrew'
Dasa	Russian Intelligence Service	1996–1999	Purchase and forwarding of armaments-related documents drawn up by a Munich arms firm (according to SZ of 30.05.2000: Arms firm Dasa in Ottobrunn)	2 Germans working on behalf of the Russians	Obtaining information on guided missiles, armaments systems (anti-tank and anti-aircraft missiles)	SZ / 30.05.2000: '(...) Betrayal of secrets not particularly serious' from a military point of view. The court ruled that this also applied to the economic damage suffered

Embargo	FIS	Around 1990	Resumption of exports of embargoed technology to Libya (e.g. by Siemens)	Interception of phone calls	Uncovering illegal arms and technology transfers	No tangible consequences. Deliveries not prevented
Enercon	Wind power expert from Oldenburg, Kenetech employee	Not stated	Wind-power plant developed by Enercon, a firm located in Aurich	Not stated	Not stated	Not stated
Enercon	NSA	Not stated	Wind wheel for generating electricity, developed by Aloys Wobben, an engineer from East Frisia	Not stated	Forwarding technical details of Wobben's wind wheel to a US firm	US firm patents the wind wheel before Wobben; (breach of patent rights)
Enercon	US firm Kenetech Windpower	1994	Important details of a high-tech, wind-powered electricity generating plant (from switch gears to sails)	Photographs	Successful patent application in the US	Enercon abandons plans to enter the US market

Enercon	Engineer W, from Oldenburg, and US firm Kenetech	March 1994	Type E-40 wind-powered electricity generator developed by Enercon	Engineer W passes on details of the generator, Kenetech employee photographs the plant and some electrical components	Kenetech seeking evidence for legal action against Enercon for breach of patent rights on the grounds that Enercon had obtained commercial secrets illegally. According to an NSA employee, detailed information concerning Enercon was passed on to Kenetech via ECHELON	Not stated
Enercon	Kenetech Windpower	Before 1996	Data concerning Enercon's wind-powered electricity generating plant	Kenetech engineers photograph the plant	Kenetech builds a copy of the plant	Enercon vindicated; legal action brought against the spying; estimated losses: Several hundred million DM
Japanese Trade Ministry	CIA	1996	Negotiations on import quotas for US cars on the Japanese market	Hacking the computer system of the Japanese Trade Ministry	US negotiator Mickey Kantor should accept lowest offer	Kantor accepts lowest offer

Japanese cars	US Government	1995	Negotiations on the import of Japanese luxury cars Information on the emissions standards of Japanese cars	COMINT, no detailed information	Obtaining information	Not stated
López	NSA	Not stated	Videoconference involving VW and López	Information intercepted from Bad Aibling	Forwarding of information to General Motors and Opel	The operation allegedly provided the State Prosecutor's Office with 'very detailed evidence' for its investigation
López	López and three staff	1992–1993	Papers and information concerning research, planning, manufacturing, and purchasing (documents concerning a plant in Spain, cost details for various models, project studies, and purchasing and saving strategies)	Collecting information	Use of General Motors documents by VW	Out of court settlement. In 1996, López resigns as VW manager, pays US$ 100 m to GM/Opel (supposedly lawyers' fees) and purchases spare parts over a seven-year period, for a total of US$1 bn

López	NSA	1993	Videoconference between José Ignacio López and VW boss Ferdinand Piëch	Videoconference recorded and forwarded to General Motors (GM)	Protection of commercial secrets held by GM in America, which López planned to pass on to VW (price lists, secret plans for a new car plant and a new small car)	López is exposed. In 1998, criminal proceedings are halted in return for payment of fines. No consequences in terms of NSA
Los Alamos	Israel	1988	Two employees of the Israeli nuclear research programme hack into the central computer of the Los Alamos nuclear weapons laboratory	Hacking	Obtaining information about new fuses for US atomic weapons	No specific consequences, as the hackers fled to Israel. One briefly held in custody in Israel, no links with the Israeli Secret Service are officially confirmed
Smuggling	FIS	1970s	Smuggling of computers into the GDR	Not stated	Uncovering of technology transfer to the Eastern Bloc	No tangible consequences. Deliveries not prevented
TGV	DGSE	1993	Cost calculation by Siemens Contract to supply high-speed trains to South Korea	Not stated	Price offer is lowered	The manufacturer of the ICE loses the contract to Alcatel-Alsthom

TGV	Unknown	1993	Cost calculation by AEG and Siemens concerning a government contract to supply South Korea with high-speed trains	Siemens claims the telephone and fax connections in its Seoul office are being tapped	Negotiating advantage for the Anglo-French competitor, GEC Alsthom	South Korea decides in favor of GEC Alsthom, although the German offer was initially considered to be better
Thomson-Alcatel v Raytheon	CIA/ NSA	1994	A Brazilian contract for the satellite monitoring of the Amazon Basin (US$ 1.4 bn) awarded to French firm Thomson-Alcatel	Interception of communications to and from the successful tenderer (Thomson-Alcatel)	Uncovering of corruption (payment of bribes)	Clinton complains to the Brazilian Government; under pressure from the US Government, the contract is awarded to US firm Raytheon
Thomson-Alcatel v Raytheon	US Department of Commerce ('made efforts')	1994	Negotiations on a project worth billions of dollars concerning the radar monitoring of the Brazilian rainforest	Not stated	Win contract	The French firms Thomson CSF and Alcatel lose the contract to Raytheon

Thomson-Alcatel v Raytheon	NSA Department of Commerce		Negotiations for a project worth US$ 1.4 bn concerning monitoring of the Amazon Basin (SIVA) Discovery that the Brazilian selection panel accepted bribes. Comment by Campbell: Raytheon supplies equipment for the Sugar Grove interception station	Surveillance of negotiations between Thomson-CSF and Brazil, and forwarding of findings to Raytheon Corp.	Uncovering bribery Winning of the contract	Raytheon wins the contract
Thyssen	BP	1990	Million-dollar gas and oil drilling contract in the North Sea	Interception of faxes sent by the successful tenderer (Thyssen)	Uncovering corruption	BP brings an action for damages against Thyssen
VW	Unknown	'recent years'	Not stated	Inter alia, infrared camera, fixed in a mound of earth, which transmits images via radio	Obtaining information about new developments	VW admits profits losses totaling hundreds of millions of deutschmarks
VW	Unknown	1996	VW test circuit in Ehra-Lessien	Hidden camera	Information about new VW models	Not stated

Source: Temporary Committee on the ECHELON Interception System. REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)). 2001.7.11.

Appendix 2: Cases of US Sanctions and Oppressing Key Companies in Other Countries

Case	Who	When	How	Aim	Consequences
Hitachi Mitsubishi Electric Corporation	FBI	1982–1983	FBI agents released false information, claiming to have the latest IBM computer technology, in order to trick Hitachi and Mitsubishi Electric employees into making a purchase.	Protect the US leadership in the field of computer.	FBI quickly arrested 6 "commercial spies" and issued a wanted poster for 12 Japanese employees. Hitachi and Mitsubishi Electric signed an IBM technology payment contract. In 1983 alone, Hitachi paid about 10 billion yen.
Toshiba Machine	SIA USTR	1981–1985	Claiming that Toshiba Machine illegally exported to the Soviet Union; investigation of Toshiba Machine; economic sanctions on Japan	Maintain America's leadership in high-tech industry	The president of Toshiba Machine and both the president and chairman of Toshiba Corporation resigned. Toshiba Corporation cancelled its contract with the US and assumed corresponding losses.
Alstom SA	DOJ FBI	2013	Former Alstom SA executive Pierucci accused of commercial bribery by DOJ, arrested by the FBI, and fined $772 million	The US maintains all French nuclear power plants	Alstom SA executives began cooperating with the DOJ and sold three-quarters of its business, to General Electric

TikTok	US government	2019–2020	Fabricate TikTok's security threat and force the acquisition of TikTok through an executive order	Suppress Chinese companies' overseas markets, especially the US market	To be determined
DJI	US government	2017–2019	The US Army bans the use of DJI UAVs and related software systems; DJI excluded from the "10 All-Around UAV Project"	Suppress China's drone technology industry	The US, Canada, and a number of other countries still use large numbers of DJI UAVs Other consequences to be determined
Huawei	DOJ BIS	2018–2020	The DOJ adds Huawei to the Entity List; Restrict Huawei from purchasing US technology and software; Prohibit the use of American chips	Suppress China's high-tech industry	To be determined
Nord Stream 2	US government	2019–2020	Trump signed the National Defense Authorization Act for Fiscal Year 2020, imposing sanctions on construction companies involved in the "Nord Stream 2" project	Prevent the US LNG market in Europe from being replaced by Russia	European countries, headed by Germany, strongly oppose the action, but the US continues to harass and threaten. Other consequences to be determined
SenseTime	DOJ	2019	The US government adds SenseTime to the Entity List	Competing with China for leadership in the field of AI technology	No significant short-term consequences

					Other consequences to be determined
Kaspersky	DHS	2017–2018	DHS requires government agencies to replace Kaspersky software within 3 months	Suspected that Kaspersky has ties to the Russian intelligence agency. Squeezed the company out of the world IT market.	Difficult to implement as Kaspersky code has already penetrated the computer infrastructure of the US government. Kaspersky is planning to spend $12 million to move its server and software business from Moscow to Switzerland
Siemens AG	US government	2018	The US asked Iraqi Prime Minister Abadi to abandon cooperation with Siemens, using "bilateral relations" as a threat.	Strengthen US influence in Iraq	General Electric replaced Siemens and obtained a $15 billion reconstruction project for Iraqi power system
TürkAkım	US government	2019–2020	Trump signed the National Defense Authorization Act for Fiscal Year 2020, imposing sanctions on "TürkAkım"	Expand the US share in the European natural gas market while limiting Russia’s share	No tangible consequences TürkAkım successfully began production in January 2020
Telefonaktiebolaget LM Ericsson	DOJ SEC	2019	According to the Foreign Corrupt Practices Act, the US government investigates Ericsson through monitoring, espionage, and searches	Hinder Ericsson's entry into the US 5G market	Ericsson pleads guilty to bribery and agrees to pay a fine of more than $1 billion

Samsung Group	US government	2012–2016	US court lists permanently banned Samsung smartphone models: Dmire, Galaxy Nexus, Galaxy Note, Galaxy Note 2, Galaxy S2, Galaxy S2 Epic 4G Touch, Galaxy S2 Skyrocket, Galaxy S3, Stratosphere	Protect Apple's patents	Samsung compensates Apple for $548 million; The US District Judge agreed to permanently ban the sale of 9 Samsung smartphone models.

Source: Compiled by the authors

编辑部：**复旦大学发展研究院**
EDITORIAL DEPARTMENT: **FUDAN DEVELOPMENT INSTITUTE**

Address: Think Tank Building, Fudan University,
No. 220 Handan Road, Shanghai, China
Post code: 200433
Tel: 86-21-55670203
Email: fdifudan@fudan.edu.cn
Website: http://fddi.fudan.edu.cn