

网络和数字外交

2023 年 5 月 12 日

中国网络体系内部—— 中国网络安全形势

海伦·普莱尔



中国网络安全治理机构架构的特点是，在国家主席习近平主持的中央网络安全和信息化委员会的领导下，参与主体和机构众多。

中国的目标是成为“网络超级大国”和技术领导者。为了实现这些战略目标，自 2012 年以来，数字技术的政策重点显著提高，并建立了**全面的网络治理制度框架**。此前，这一政策领域支离破碎，分散在许多不同的机构中。现在，该系统由众多党和国家机构、附

属（表面上是非政府的）智库或研究机构以及技术实体、行业协会和行业联盟组成。以下博客文章说明了中国网络安全格局的底层结构，并介绍了主要参与者，特别是引用了 **Rogier Creemers** (2021) 的一篇论文，他在其中追溯并进一步阐述了这些机构的重组。

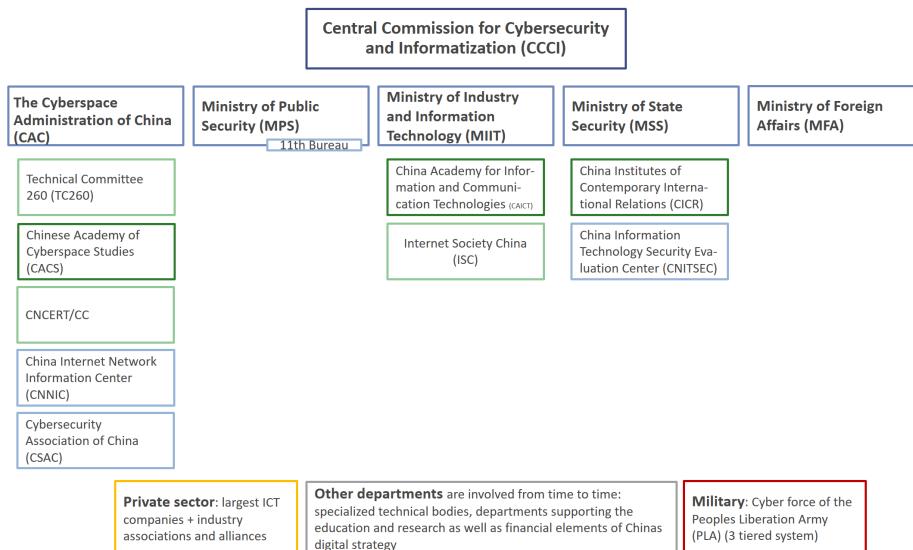


图 1：机构网络治理框架图解。

中国的网络政策由习近平亲自自上而下指挥，他担任中央网络安全和信息化委员会主席。中央网络安全和信息化委员会是中国政府最强大的机构之一。其职责包括提供领导和部门间协调、协调**国防和私营部门的融合**、促进决策以及解决网络安全和信息化领域的部门间紧张关系。然而，该委员会的运作大多是秘密进行的。

金字塔的下一层是国家互联网信息办公室 (CAC)，它是中国网络安全和关键信息基础设施管理委员会的主要工作机构，并提供行政支持。其职责以协调为主，包括指定网信办为网络安全审查和关键信息基础设施管理的主管部门，领导网络个人数据保护部门，共同管理数据安全，起草国家网络空间安全战略。此外，网信办还负有监管责任，负责网络内容控制和网络运营商的相关许可手续。因此，它监督五个下属组织：技术委员会 260 (TC260) 负责技术信息安全标准。据估计，**自 2015 年以来**，TC260 已发布了约 300 项此类标准。从官方角度来看，它是一个独立机构，但与网信办有明显的联系。它由七个定期工作组组成，专注于不同的网络安全问题。外国公司可以参加其中一些工作组，但其他一些工作组仅供中国官员和中国科技公司代表参加。这些标准带来了诸多挑战，使**外国公司在中国开展业务变得越来越困难**。中国网络安全协会 (CSAC) 也受国家网信办监管。它是一个中介组织，协助政府部门有效实施法律、法规和政策。网信办还负责监管下属智库中国网络空间研究院 (CACS)。该研究院不开展国际业务，但每年发布中国和世界各地互联网发展报告。网信办还负责

监管 CNCERN/CC，该中心的任务是应对网络攻击，预防、检测和应对漏洞和事件。此外，它还参与国际事务，自称是一个非政府技术中心，但与政府机构联系密切。中国互联网络信息中心(CNNIC)也属于网信办管辖范围，负责监管.cn 顶级域名和普通话域名的 DNS 技术运营。

中国的网络安全重点主要来自中共维持其权力控制的主要目标。因此，内容控制发挥着重要作用：公安部 (MPS) 负责发布有关如何报告或审查特定类型信息的直接指示。它指挥中国警察部队，负责执行法律法规，并针对高优先级问题开展有针对性的活动。例如，它监督“金盾工程”和国家信息安全管理系統，即“**长城防火墙**”。长城防火墙是“金盾工程”的一部分，于 2000 年启动。它描述了中国政府的互联网审查和监视项目，该项目包括审查机制和宣传元素，旨在限制内容，例如封锁某些外国网站、识别和定位个人以及提供对其个人信息的访问。**金盾项目**与防火墙共享硬件和软件，但处理国内执法问题，并构成可与社会信用体系挂钩的数据庫。此外，第十一局还负责监督网络安全等级保护系統 (MLPS) 的运行，以保障信息安全并打击网络犯罪。

工业和信息化部 (MIIT) 负责网络基础设施的建设和管理，包括部署 5G 技术，以及相关的信息安全任务，此外还负责制定 ICT 行业的产业政策。因此，它在互联网和电信基础设施方面发挥着重要作用。它负责监督中国信息通信技术研究院 (CAICT) 和中国互联网协会 (ISC)。这两个机构都自称是非政府机构，并声称是独立的。CAICT 是一个智库，负责研究和政策制定、发布出版物，并为行业和政府提供意见，例如技术标准。因此，它在 ICT 政策和标准的制定中发挥着作用，特别是作为外国 ICT 公司在这些问题上的重要对话者。另一方面，ISC 是互联网行业的中介组织，有 16 个工作组处理从网络版权保护和农村信息化到垃圾短信和互联网金融等问题。在国际上，ISC 自我定位为中国数字环境的非政府、多利益相关方组织，但实际上它发挥着监管作用。

尽管努力重组机构格局，使责任不再分散在许多不同的机构，但网络安全和隐私的官僚职责**仍然多种多样且相互冲突**，网信办、工业和信息化部、公安部、TC260 和网信部门在标准、法规和实施方面都有一些发言权。

在国际舞台上的外部问题上，国家安全部 (MSS) 对中国的网络外交和网络安全议程的实施至关重要。尽管关于中国情报和安全机构的公开信息很少，但它被怀疑与 APT3、APT10 等**黑客组织有关联**。MSS 监管两个机构：中国现代国际关系研究院 (CICR) 和中国信息技术安全测评中心 (CNITSEC)。CNITSEC 收集有关软件和硬件产品以及信息系统的漏洞信息。它管理中国国家信息安全漏洞数据庫 (CNNVD)，并执行 CSL 及其下属法规规定的安全审查流程。CICR 声称自己是一个专注于国际事务的研究机构，但它与 MSS 关系密切，其许多高级领导人都有情报背景。它是负责国际上 1.5 轨和 2 轨关系的主要机构。

最后，外交部 (MFA) 负责参与该领域的国际网络外交进程。然而，**与其他专题领域一样**，外交部对网络相关政策的直接权力非常小。

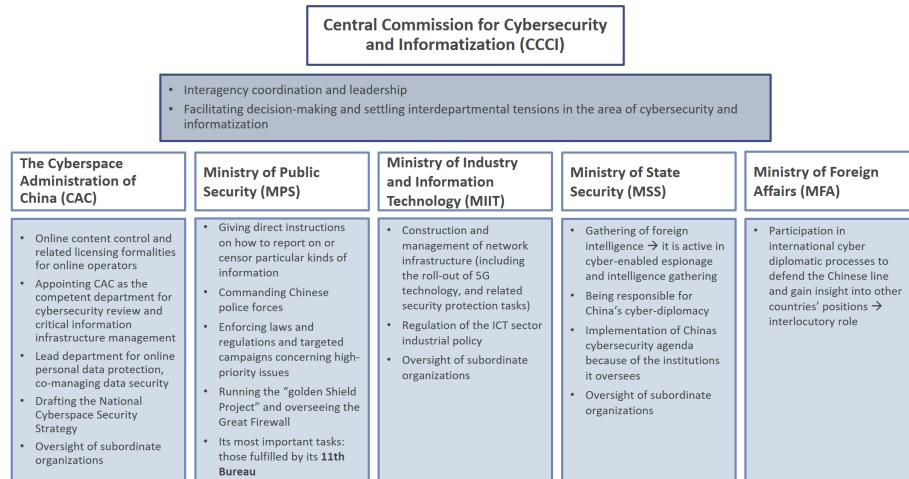


图2：各机构任务概要。

此外，其他部门也时常参与网络问题：专门技术机构、支持教育和研究的部门以及中国数字战略的财政部门。此外，尽管中国的数字技术政策在很大程度上是民事特权，但它与解放军的能力和理论日益交织在一起。例如，解放军**网络部队也是一个主要参与者**，在国外开展网络行动，在国外从事经济间谍活动，或与各种APT密切联系。它还将网络空间行动视为**信息战的重要组成部分**。

综上所述，中共在很大程度上参与了网络治理体系的各个阶段。而且，网络治理体系的重组和扩展也基本完成。但是，不能排除新的发展以及官僚机构和关键技术领域的升级：例如，一个**新的数据管理机构**在2023年初才作为国务院进一步重组的一部分成立。它将负责协调和推动数据要素体系的建设，统筹数据资源的综合共享、开发和利用，统筹推进数字中国、数字经济和数字社会的规划建设。这样，数据将作为“第五大**生产要素**”。此外，同样在政府安全担忧的驱动下，技术“本土化”的目标更加被强调（目标是到2035年实现技术自给自足并成为世界顶级创新者）。为此，国家**创新和研究正在日益得到推动**。预计新政府将加强科技部（MoST）在追求科技成功方面的监督和政策作用。

此外，**私营部门在中国网络安全领域也发挥着重要作用**，尤其是阿里巴巴、百度和腾讯等最大的ICT公司以及行业协会和联盟。它们处于中国全球技术雄心的前沿，尤其是在中国制定标准、影响全球数字秩序和实现技术自力更生的国际网络雄心方面。因此，它们也对国内ICT政策具有重大影响。

最后，治理体系由**相互关联的政策、法律、政策、法规和标准**组成，使其成为“世界上任何国家中网络空间和信息通信技术(ICT)

最全面的治理体系”。虽然《网络安全法》是最核心的，但**它因允许广泛的数据控制和增加知识产权盗窃风险而受到批评**。此外，其措辞和定义相当模糊，增加了政府对调查需要做出广泛声明的理由，并降低了外国公司挑战政府数据访问要求的能力。所有这些文件都涉及数字经济以及安全问题，例如安全审查、关键基础设施保护、在线内容管理、加密和数据流。这种治理体系使中国有机会与**欧洲并驾齐驱**，拥有强大的数据和安全治理模式。其他国家甚至正在采用与中国类似的法律，从而带来了传播和加强独裁政权的风险。

此外，**乌镇互联网大会**自2014年起每年举行一次，是中共宣传网络问题理念的重要平台。该会议用于讨论互联网问题和政策，旨在为各国提供建立自己的网络空间规则的机会，正如习近平在会议上提出的**网络主权概念**。这种理解与目前西方占主导地位的自由互联网观念背道而驰，因为它将允许各国在数字空间拥有最终权威。它将在网络空间建立国家边界，阻止信息的自由流动，使互联网更容易被控制，并实现“数字威权主义”。因此，中国正寻求在全球层面按照自己的理念塑造网络空间，例如通过联合国进程，例如2011年**向联合国提出的“信息安全国际行为准则”提案**，或在2019年**互联网电信联盟会议上提出的“新IP”**等提案。

我们正目睹中国作为科技强国的快速崛起：其能力在不断增强，但尚未占据主导地位。北京的雄心也有其**局限性**：缺乏人才和创新来实现这些战略目标，而且对外国技术的依赖程度很高。中国政府为克服这些障碍采取的一项措施是2017年成立**国家网络安全中心**。它由七个研究、人才发展和创业中心组成。克服这一挑战并实现成为网络超级大国的愿望的另一个重要方面是经济外交工具和中国科技公司的全球活动，例如“数字**丝绸之路**”。中国科技公司在这方面发挥着越来越重要的作用。这些项目是由寻求新市场的中国公司推动的，并支持政府获得经济、战略和政治影响力的雄心。出于这些原因，政府为这些公司及其创新项目**提供财政支持并投入巨资**，主要关注5G、AI和半导体等新兴技术。

此外，新政府更加重视（国家）安全和控制，这也会影响技术政策。ASPI最近的一份**报告**警告说，尽管中国尚未拥有技术优势，但它已经在人工智能等广泛领域主导未来关键技术奠定了基础。这一预测似乎是合理的，因为创新和技术自给自足是中国的战略重点，正如**习近平主席**在2018年所说：“自主创新是必由之路……要成为世界技术领先者。”概述的网络治理制度是实现所有这些目标的基石。因此，了解它对于分析中国作为网络空间参与者及其野心至关重要。



海伦·普莱尔

数字社会研究所 (DSI) 研究助理

+49 30 212 31-1654

helene.pleil@esmt.org

快速链接

› [更多 DSI 博客文章](#)

文章选项

[通过邮件发送](#)

[通过 Facebook 分享](#)

[通过 Twitter 分享](#)

[通过 Linkedin 分享](#)

添加新评论

你的名字 *

电子邮件 *



评论 *

//

节省

信息

ESMT 博士研究
学位课程
高管教育
图书馆/信息中心
工作
English 网站

联系我们

ESMT Berlin
Schlossplatz 1
10178 Berlin, 德国
电话: +49 30 212 31
○
info@esmt.org

通讯

随时了解学校周边的信息和活动。

报名

[法律声明](#) [一般条款](#) [資料保隱](#) [隐私设置](#)

