

# 跨国网络犯罪治理中公私合作的主要困境及出路

刘镇蒙

北京外国语大学法学院硕士研究生，北京

发布日期：2026年8月24日

## 摘要

在全球数字化浪潮的推动下，跨国网络犯罪智能化、隐蔽化和全球化趋势不断凸显，对国家安全和社会稳定构成了严重威胁。依靠公共部门的传统治理模式已难以应对复杂多变的网络犯罪形态，公私合作模式因其资源整合和技术优势逐渐成为跨国网络犯罪治理的重要路径。然而，当前该模式在实践中面临数据主权争议、跨境执法冲突、法律制度滞后、企业合规压力和信任缺失等多重障碍。有鉴于此，本文深入剖析了我国公私合作机制在实际运用中所面临的主要困境，提出了构建全球数据治理框架、完善跨境数据共享机制、健全法律与合规体系和重塑公私信任关系等可行性对策，为我国完善跨国网络犯罪治理体系、提升数字治理效能提供了理论支撑和实践路径。

## 关键词

跨国网络犯罪；公私合作；数据主权；法律规制；协同治理

# Public-Private Cooperation in Transnational Cybercrime Governance: Major Dilemmas and Solutions

Zhenmeng Liu

Postgraduate Student, School of Law, Beijing Foreign Studies University, Beijing 100089, China

## Abstract

Driven by the wave of global digitization, transnational cybercrime is becoming increasingly intelligent, hidden and globalized, posing a serious threat to national security and social stability. The traditional governance model relying on the public sector is no longer able to cope with the complex and ever-changing forms of cybercrime, and the public-private partnership model has gradually become a significant path for transnational cybercrime governance because of its resource integration and technological advantages. However, the model is currently facing

文章引用：刘镇蒙. (2026). 跨国网络犯罪治理中公私合作的主要困境及出路. 法学年鉴, 1(3), 1 - 19.

ISSN Print: 3079-5389, ISSN Online: 3079-5397.

DOI: 10.63313/Law.8023

multiple obstacles in practice, such as data sovereignty disputes, cross-border law enforcement conflicts, lagging legal systems, corporate compliance pressure and lack of trust. In view of it, this paper deeply analyses the main dilemmas faced by China's public-private partnership mechanism in practice, and puts forward feasible countermeasures such as constructing a global data governance framework, perfecting the cross-border data sharing mechanism, sounding the legal and compliance system, and reshaping the relationship of public-private trust, etc., so as to perfect the transnational cybercrime governance system for China. This study provides theoretical support and practical paths for China to improve its transnational cybercrime governance system and enhance the effectiveness of digital governance.

## Keywords

Transnational Cybercrime; Public-private Partnership; Data Sovereignty; Legal Regulation; Collaborative Governance

Copyright © 2026 by author(s) and Erytis Publishing Limited.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



## 一、跨国网络犯罪治理中公私合作相关问题概述

### （一）网络犯罪治理中的公私合作模式

公私合作模式（Public-Private Partnership, PPP）是指公共部门与私营部门之间为了共同的目标而进行的合作。这种合作形式涵盖了从项目策划、实施到管理的全过程，强调双方的平等互利和资源共享。在网络犯罪治理中，公私合作模式的目的是确保各利益相关方能够以最大的自主性和主动性参与网络犯罪的治理，构建一个“多主体参与、多层次协同”的治理架构。这一模式具有灵活性和适应性，在网络犯罪治理中具有显著优势，能够及时应对网络犯罪的快速变化，通过多主体参与和多层面协同，全面覆盖网络犯罪各个方面，提升治理的效率和效果。

#### 1. 国际实践

在国际层面，公私合作模式在网络犯罪治理中得到了广泛的应用。美国白宫在 2023 年 3 月发布的《国家网络安全战略》中指出，公共部门与私营部门需携手建立长期稳定的伙伴关系，携手打造坚固的网络安全屏障。美国土安全部的关键基础设施伙伴关系委员会（Critical Infrastructure Partnership Council, CIPAC）支持下的持久安全框架，是一个由美国国防部和国防工业基础（U.S. DIB）组成的公私合作组织，旨在应对共同的网络安全威胁。日本已搭建起执法部门与互联网企业协同工作的框架，并明确了一系列指导原则来规范双方的合作方式。挪威借助“网络安全中心”这一平台，为执法机构与互联网企业提供了合作契机，增强了双方在调查网络犯罪方面的协作经验。白俄罗斯制定了专门的指导文件，引领公私合作开展网络犯罪治理工作，保障合作在清晰的法律框架下推进，从而提升合作效率。

#### 2. 困境与挑战

虽然公私合作模式在网络犯罪治理中具有显著优势，但也面临诸多挑战。各国国内法律规制不完善，特别是在跨境数据取证时采用公私合作模式缺少国际法基础。此外，数据安全和隐私保护的平衡问题也成为重点。在推进公私合作时，如何既确保互联网企业等私主体的合法权益和个人隐私，又能有效促进犯罪治理，已成为亟待解决的核心难题。不同国家或地区对于本国网络服务提供者能否自愿协助他国刑

事司法活动、在何种范围内协助、如何协助的规定均不相同，加之各国在数字法治方面的制度差异，网络服务提供者在协助他国刑事司法机关时可能会违反本国法律规定，因此存在公私合作的困境。

公私合作模式在网络犯罪治理中具有重要的理论和实践意义。通过整合公共部门和私营部门的资源和专业技能，形成多主体参与、多层面协同的治理体系，能够有效提升治理的效率和效果。然而，该模式也面临法律规制不完善、数据安全和隐私保护、国际协调和合作机制等挑战。未来，国际社会需要共同努力，制定更加全面和协调的国际法律文件，以应对跨国网络犯罪的挑战。

## （二）跨国网络犯罪治理中的公私合作模式

如今，互联网全球化深入发展，跨国网络犯罪（Transnational Cybercrime）已成为一种全球性威胁。这类犯罪通常跨越多个国家，涉及不同地区的法律、文化、技术等因素，传统的单一国家或地区的治理手段往往无法有效应对，而公私合作模式能够有效破除这一困境，通过整合公共部门和私营机构的资源、技术和信息，形成合力以应对跨国网络犯罪带来的多方面挑战。

### 1. 公私合作模式的定义与理论框架

公私合作模式指的是公共部门与私营部门之间为实现共同目标而进行的合作。这种模式强调双方的互利合作和资源共享，尤其在跨国网络犯罪治理领域，公私合作模式具有显著优势，主要包括以下几点：

第一，该模式具有灵活性与适应性。在跨国网络犯罪快速发展的背景下，公私合作模式能够通过快速反应和灵活调整应对不断变化的网络威胁。第二，多主体参与、多层面协同。通过政府、企业和国际组织等多方共同参与，构建起多层次的治理体系，使得治理措施能够覆盖跨国网络犯罪的各个方面。第三，实现了资源整合与优势互补。公私合作能够整合公共部门的法律、政策和国际协调资源，与私营部门的技术、数据和市场资源相结合，汇聚成更为强大的治理力量。

在跨国网络犯罪治理中，公私合作模式能够充分调动全球资源，加强国际合作，提高反应速度和精准度，有效应对层出不穷的犯罪形式。

### 2. 公私合作模式的国际实践

美国是公私合作模式在网络犯罪治理中的典型实践者。美国政府高度重视与私营部门的合作，尤其是在网络安全领域。2023年3月，美国白宫发布的《国家网络安全战略》明确指出，公共部门与私营部门需要建立持续的合作伙伴关系，共同构建强大的网络安全防线。例如，美国国土安全部下属的关键基础设施合作委员会（CIPAC）就是一个由政府与私营部门（特别是国防工业基础）组成的合作组织，旨在应对共同的网络安全威胁。日本在网络犯罪治理中也积极推动公私合作。日本的执法机关与互联网公司之间建立了稳定的合作机制，并制定了明确的合作指导原则。这一机制不仅确保了信息共享，还提高了执法机关在面对复杂网络犯罪时的应对能力。

部分国家为此设立了专门机构，以确保高效响应及时惩治跨国网络犯罪的需要。如挪威设立了“网络安全中心”，为执法机关与互联网企业之间的合作提供了有力支持。这一中心为跨国网络犯罪的调查提供了平台，帮助提升了跨国公私合作的经验和效率。还有部分国家专门针对公私合作模式制定了相关法律法规，以准确指导关联主体如何运用公私合作机制，解决适用障碍，如白俄罗斯通过出台专门的法规，明确了公私合作在网络犯罪治理中的合法性和操作流程。这些规定确保了跨国合作能够在法律框架内顺利进行，提高了治理的效能。

### 3. 公私合作模式的法律规制

#### （1）国际法律框架

随着跨国网络犯罪问题的日益严重，国际社会已经开始推动建立统一的法律框架。2024年12月24日，《联合国打击网络犯罪公约》的通过，为全球范围内打击网络犯罪提供了系统性的法律支撑。该公

约不仅涉及立法、罪名确立、程序权力、国际合作等方面，还特别关注技术合作、性别考量、隐私保护等内容，旨在通过加强国际刑事司法合作应对跨国网络犯罪。

### （2）国内法律体系

不同国家对于公私合作模式的法律创制和法律适用存在差异，尤其是在某些情境下，例如跨境数据取证过程中运用公私合作机制，国际法基础的缺失问题尤为突出。除此之外，还包括其他情形。以俄罗斯为例，俄罗斯刑法明确规定网络犯罪包括通过计算机网络实施的犯罪，而对数据隐私保护有严格要求。此类法律层面的差异可能对跨国网络犯罪治理产生一定影响，因此，国际法律协调显得尤为重要。

### （3）法律冲突与协作难题

跨国网络犯罪治理中，由于国家间法律制度差异和对隐私保护的不同立场，导致了国际刑事司法合作中的法律冲突。例如，某些国家可能限制或禁止将其境内的网络数据共享给他国执法机关，阻碍合作的顺利进行，而解决这一问题则需要在全球范围内协调和统一各国法律规范。

## 4. 数据安全与隐私保护

在跨国网络犯罪治理中，数据安全和隐私保护始终是一个核心问题。私营部门（如互联网公司、技术企业等）在协助政府打击网络犯罪时，如何平衡数据共享与保护用户隐私，尤其是在跨境数据传输和取证过程中，需要满足严格的合规要求。不同国家对数据隐私的保护规定差异较大，进行国际刑事司法合作时需要考虑到以下两个主要问题：其一，数据隐私的跨境传输。一些国家对数据跨境流动有严格的控制，例如欧盟的《通用数据保护条例》（GDPR）就对数据传输设定了严格的规则，要求数据传输方必须确保数据的安全性和隐私性。其二，隐私保护与执法冲突。某些国家的法律规定要求互联网企业提供用户数据以协助跨国司法调查，而这些企业可能同样面临本国法律针对数据保护和隐私权等敏感问题所施加的限制。因此，跨国网络犯罪治理中，如何在全球范围内制定统一的数据安全规则和隐私保护框架以及相应的跨境合作机制，是一个亟待解决的难题。

## 5. 国际协调与合作机制

### （1）国际合作机制

网络犯罪的跨国性决定了它无法仅仅依赖单一国家的法律或制度进行治理。为此，国际间的法律法规、政策协调和合作机制显得至关重要。在加强国际合作，深化各国政治互信的前提下，各国能够共同创建和完善打击跨国网络犯罪的机制。目前，联合国、国际刑警组织（Interpol）和欧洲刑警组织（European Police Office, Europol）等国际组织在跨国网络犯罪治理方面发挥了重要作用。其中，国际刑警组织与私营部门的合作，已成为全球范围内打击网络犯罪的重要组成部分。

### （2）全球性治理模式

为有效实现跨国网络犯罪治理需要建立全球性国际协调机制，确保各国之间能够及时分享情报、技术和司法合作资源。中国一直建设性参与《联合国打击网络犯罪公约》谈判，以网络空间命运共同体理念为引领，倡导在全球范围内建立高效有力的打击网络犯罪合作机制，与金砖国家等广大发展中国家密切配合，并同西方国家保持沟通协调，为最终推动《公约》的达成发挥了重要作用。因此，国际合作应建立在全球各国公平、公正参与以及平等协商的基础上，确保网络空间的安全与秩序。尤其是对于发展中国家来说，推动跨国治理和加强国际合作能力建设，将成为全球网络空间治理中的关键一步。

总之，跨国网络犯罪治理中的公私合作模式为应对这一复杂、全球性的问题提供了新思路。通过公共部门和私营部门的紧密协作，能够有效整合资源、共享信息、加强技术支持，确保跨国网络犯罪治理提质增效。然而，公私合作模式在实践中仍面临法律规制不完善、数据隐私保护、跨国合作协调等挑战。国际社会需要进一步推动法律框架的完善，加强对话沟通、促进资源共享，构建更为强大的跨国治理体

系。随着全球范围内网络安全威胁的不断升级,公私合作模式将在网络犯罪治理中发挥愈加重要的作用。

## 二、跨国打击网络犯罪公私合作的主要障碍

根据《2024 年最高人民检察院工作报告》,全国检察机关共办理各类案件 425.3 万件,同比上升 28.9%。其中,制定检察机关网络法治工作 21 条意见,起诉利用网络实施的犯罪 32.3 万人,同比上升 36.2%, 超过 2023 年全年所办理案件总数的同比增长率。从 1 月 13 日召开的全国检察长会议上获悉,2024 年 1 至 11 月,起诉电信网络诈骗犯罪 6.7 万人,同比上升 58.5%。最高检与最高法、公安部共同印发《关于办理跨境电信网络诈骗等刑事案件适用法律若干问题的意见》,依法打击跨境电信网络诈骗犯罪,积极参与打击治理涉缅北电诈犯罪专项行动,最高检指导地方检察机关依法对缅北明家犯罪集团 39 人提起公诉。检察机关依法惩治网络谣言、网络暴力等相关犯罪,用法治力量维护网络清朗,2024 年 1 至 11 月,检察机关起诉利用网络实施的犯罪 24.2 万人。

如今,社会正遭遇全方位犯罪的网络化浪潮,网络技术的迅猛进步也催生了网络犯罪手法的持续创新。在这样的形势下,研究网络空间国际治理框架下的公私合作模式显得尤为关键且契合时代需求,这不仅关乎跨国网络犯罪治理的成效,还可能在更根本的层面波及刑事司法的运行机制。跨国网络空间犯罪的治理确实遭遇诸多棘手难题。一方面,刑事司法管辖权的归属常引发各国主权的碰撞;另一方面,网络技术的飞速变革带来了技术差距,这无疑加大了治理的复杂性。此外,传统刑事诉讼法的基本原理、理念、价值和构造在应对跨国网络空间犯罪时显得力不从心,无法完全满足打击此类犯罪的需求。这些挑战不仅考验着各国的法律和技术能力,也对国际合作提出了更高的要求。面对网络犯罪的全球性挑战,国际社会已进行了多次立法尝试,其中具有代表性的包括联合国大会于 2024 年通过的《联合国打击网络犯罪公约》(UN Convention against Cybercrime)、《布达佩斯公约》(Budapest Convention on Cybercrime)(正式名称为《网络犯罪公约》)、美国《澄清合法使用境外数据法》(简称为《云法案》)(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)机制、欧盟《一般数据保护条例》(General Data Protection Regulation, GDPR)和《涉刑事电子证据提取和存留命令条例》(Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters)以及非洲联盟的《马拉博公约》(Malabo Convention)等。在国际立法探索过程中,强调网络信息业者在对抗跨国网络犯罪时的重要作用,并着力推动建立跨国网络犯罪治理的公私合作模式,是国际社会普遍认可的理念。鉴于平台型组织在数字社会中作为关键纽带和核心场所的角色,传统的自上而下的单一保护型管理模式往往难以应对数字化平台的复杂架构。有鉴于此,愈来愈多的国家倾向于采用公私合作模式,促使平台在社会治理中更积极主动地发挥作用,依法配合监管机构的指导,采取有效措施保障公民合法权益。

综上,无论是国外还是国内,无论是从法律理论还是实际操作层面来看,公私合作模式都已成为治理跨国网络犯罪的重要方式。然而,即使该模式存在诸多优势,但在利用其进行犯罪治理时,也必然会遭遇困境。只有正视困境和挑战,才能找到正确方法以完善跨国网络犯罪治理的公私合作模式,为全球网络安全的维护作出更大贡献。

### (一) 数据主权争议与跨境管辖权对立

在跨国打击网络犯罪过程中,跨境取证是侦查活动的关键环节,必然涉及数据主权和国家安全,各国正通过法律手段加强境内数据管控,且力图使用位于他国境内的各项数据。而跨国向别国网络信息业者调查取证实际上是以取证对象的管辖连接点取代了证据材料的管辖连接点,而这必然会引发与数据所在国的主权冲突。

在大数据时代背景之下，数据的战略价值不容小觑，各国围绕数据主权的博弈愈演愈烈，尤其是在数据跨境流动背景下，传统国家主权概念也在不断演变，“数据主权”逐渐成为主权热点。这一概念不仅涉及一国对境内数据的控制权，也延伸至国家对境外数据的潜在使用权。各国都在不同程度上通过政策和法规强化对本国数据的控制，以维护其在国家安全、经济利益和政治利益等方面的主权。这就势必造成跨境数据管辖权的极大冲突。

2007年，比利时警方侦查到一起网络诈骗案件，发现嫌疑人主要通过位于美国的雅虎邮箱联系。比利时检方请求雅虎提供涉案邮箱注册信息，以识别嫌疑人身份，但雅虎拒绝配合，理由是美国《电子通信隐私法》不允许该种数据被分享。比利时方面则坚持依据其国内《刑事诉讼法》要求雅虎履行数据提供义务。由此，双方展开了一场长达数年的法律拉锯战。最终，比利时最高法院裁定，尽管雅虎在比利时没有实体机构，但其电子邮箱服务在比利时构成管辖依据，因而要求雅虎提供前述邮箱信息。

该案中，数据主权博弈是核心问题。在比利时警方请求雅虎提供相关电子邮件信息时，雅虎拒绝配合并依据美国《电子通信隐私法》主张其无权分享数据。这里的核心问题是美国对其境内数据的控制权，即数据主权，与比利时司法机关试图依据其国内刑事诉讼法对雅虎施压的行为发生冲突。这种冲突正是数据主权博弈的体现：各国都试图通过本国法律来确保自己对数据的绝对控制，以维护国家安全、经济利益及政治利益。然而，跨国网络犯罪案件中的数据流动往往无法完全受限于某一国的法律体系，导致了司法管辖权上的对立。

跨境管辖权冲突在该案中也尤为突出。比利时司法机关要求雅虎根据比利时国内法提供数据，但雅虎指出其数据存储在美国，不受比利时司法管辖。雅虎提出的法律依据表明，美国的法律体系对该数据拥有优先管辖权。这一管辖权冲突的根源在于，虽然比利时司法机关具有在其国土上执行法律的权力，但由于数据被存储在美国，数据所在国的法律与数据请求国的法律在执行层面产生了对立。这种情况反映了跨境管辖权冲突的现状，尤其是在大数据时代，数据不再受限于传统国界，而是全球化流动，导致了各国法律制度的差异以及不同国家之间的法律适用冲突。

数据主权博弈和跨境管辖权冲突加剧了公私合作的困境。由于私营部门（如互联网企业）掌握着大量涉及犯罪的电子数据，因而在跨国网络犯罪侦查中发挥着至关重要的作用。然而，私营企业往往面临着来自本国和他国法律要求的双重压力。雅虎作为互联网私营企业，在遵守美国法律的同时，也需满足比利时司法机关的请求。在此情境下，雅虎处境尴尬，一方面，依据数据主权，美国法律要求其保护其所掌握的数据隐私，另一方面，国际司法合作亦要求其配合外国司法机关。这种双重压力不仅使私营部门难以顺利配合各国的调查，也暴露出公私合作机制在跨境取证等跨国网络犯罪侦查活动中的脆弱性。

公私合作的力量平衡也在此案中遭遇了挑战。尽管雅虎拥有大量数据和技术优势，能够在打击网络犯罪中发挥关键作用，但其与政府间的合作却受到严重制约，反映了数据主权与隐私保护之间的张力。私营企业在面临国家主权干预时，可能会倾向保护用户数据而非积极配合跨国侦查，而这会导致公私合作成效大打折扣，甚至无法开展。最终，比利时最高法院裁定雅虎必须向其提供所需数据，裁定结果表明了跨境数据流动中的管辖权归属，也突显了数据主权博弈对公私合作机制的挑战。这一案例揭示了在跨国网络犯罪治理过程中，公私合作模式面临的关键问题：一方面是国际刑事司法合作对私营机构数据支持的强烈需求，另一方面在于各国法律规范对数据控制权的不同主张与理念。

跨国打击网络犯罪案件中公私合作往往会引发两国之间的数据主权博弈以及跨境管辖权冲突问题。受到“数据主权”观念的极大影响，公私合作机制在跨境调取电子数据中的运行也必然受到阻碍。无论是对于一国境内的数据还是境外数据，一般而言，其控制权均牢牢掌握在公权力机关手中，国家在一定程度上以各种方式实现对数据的绝对控制；相较之下，私营部门原先所具有的资源及信息优势不复存在，

公私双方在跨国网络犯罪治理中的力量平衡将被打破，在某些情境下，公私合作名存实亡。跨境数据管辖权冲突是数字时代的必然结果，源于国家主权与数据共享需求之间的对立。各国在捍卫数据主权的同时，需要在促进全球数据流动与保障本国安全之间找到平衡。为此，国际社会应加大合作力度，制定全球数据治理的统一标准。通过优化国际法律框架和灵活应用跨境数据规范，可以更好地调和各国利益，应对数字化和全球化带来的数据流动挑战。

## （二）私营机构合规困境

合规难题主要源于以下三方面：首先，国内法律义务之间存在矛盾，突出表现为网络信息业者在协助执法和保障数据安全及个人隐私方面的冲突；其次是本国法律与外国法律义务的碰撞，这主要体现在各国在网络空间治理的政策和规则上的不同；最后是协助执法义务与商业利益的对立，这不仅关乎网络信息业者在协助执法时的商誉和商业机密保护问题，还包括运行相关机制以协助执法所产生的成本。

### 1. 国内法义务的冲突

网络信息业者在协助执法时，常常面临国内法义务的冲突。具体表现为配合执法的义务同保障数据安全和个人信息保护义务之间的矛盾。例如，私营企业可能被要求提供用户数据以协助执法，但同时又需遵守严格的隐私保护法规。这种冲突不仅影响私营企业的合规性，还可能引发用户对数据安全的担忧。企业必须在多重义务之间进行平衡，确保在协助执法的同时，不侵犯用户的隐私权益。

### 2. 国内法与国外法的义务冲突

各国在网络空间管理的策略和法规方面各有不同，这种差异使得国内法律与国外法律义务之间产生了矛盾。例如，美国的《云法案》允许美国执法机关在某些条件下获取存储在境外的数据，这与一些国家的数据主权和隐私保护法规发生了冲突。全球已有超过 340 项国际、区域、双边贸易协定包含数据跨境流动条款，其在内容和约束力上差异显著。新型数字贸易协定如《全面与进步跨太平洋伙伴关系协定》和《数字经济伙伴关系协定》通过专章形式明确提出了整套具有法律约束力的数据跨境流动原则及其执行机制，而传统型贸易协定如《韩国—秘鲁自由贸易协定》等则未设定强制性义务，允许数据流动规则的多样性和本地化。

### 3. 协助执法义务与商业利益的冲突

网络信息业者在协助执法时，还面临商业利益的冲突。一方面，企业可能因协助执法而影响商誉和商业秘密保护。例如，企业可能被用户视为侵犯隐私，从而影响其商誉。此外，企业还需要保护其商业秘密，如算法模型等，这些秘密在协助执法过程中可能被泄露。另一方面，支撑协助执法机制的成本也是一个重要问题。企业需要投入大量资源来建立和维护合规机制，包括数据安全系统、内部审查机制等。这些成本可能对企业的财务状况产生重大影响，尤其是在中小企业中。企业需要在合规成本和商业利益之间进行权衡，确保在满足法律要求的同时，不会因过度合规而影响其竞争力。

跨国打击网络犯罪中的公私合作面临着诸多合规困境，这不仅影响企业合规性，还可能引发国家间的法律冲突和政治紧张。为了有效应对这些挑战，国际社会需要在尊重彼此主权的基础上，通过多边合作和国际协议，建立更加灵活和有效的数据治理框架，促进数据的自由流动和国际合作，同时保护国家安全和公民隐私。

## （三）跨国网络犯罪治理政策的转型挑战

在欧美国家和地区，“网络适应性”（Cyber Resilience）这一政策理念在网络安全治理中被广泛提及，并逐渐取代了传统的犯罪控制或安全控制等概念。网络适应性是指指各类机构和组织在遭遇网络攻击时的抵御、监测、应对和修复能力，借助这种能力，努力将网络攻击对其商业声誉和竞争地位的损害

减至最小。与传统网络犯罪治理观念相比,该政策突出强调维护网络空间安全需覆盖网络活动的全周期,既涵盖对潜在网络风险的预防,也包括犯罪行为发生后的侦查、阻断和反击,以及遭受网络攻击后恢复计算机系统和数据的能力。这种全方位的网络预警与响应机制对网络数据共享的要求极高,要求网络参与主体必须多元化。

然而,当前实践中存在两方面问题:一方面,部分私营企业或组织过度依赖公共部门在网络安全治理中的作用,这种消极态度不利于网络安全伙伴关系的建立和信任体系的构建;另一方面,在网络黑产巡查、恶意程序工具发现、程序功能鉴定能力、非法网站排查与取缔、境外赌博、色情等非法链接拦截等方面存在监管漏洞。这两方面问题加剧了公私主体间的矛盾。在此情况下,改变传统以行政执法机构为主导的管理模式迫在眉睫,需构建一种更具包容性和多元性的网络安全管理体系。这种转变既需要政策层面的支持,也需要企业和政府之间的紧密协作。比如,私营部门需在网络安保方面承担更多责任,而公共部门则需提供必要的支持与指导。

面对全球移动终端的普及、社交媒体的影响力以及恶意软件的泛滥,国际社会急需共同正视新技术环境下网络犯罪带来的新挑战。这包括不同区域国家法律规范的滞后、缺失和差异导致新型网络犯罪的司法惩处力度不够;各国现行法律制度框架难以充分保障跨境取证的高效快捷,常使跨国网络犯罪的执法追诉陷入迟滞低效的困境;部分国家现有的监测预警和应急处置机制难以有效应对网络匿名背景下网络设备的脆弱性以及网络用户数量急剧增长的现状。

#### (四) 网络犯罪治理公私合作制度的缺失

在跨国网络犯罪治理方面,公私合作的立法存在空白。尽管存在一些区域性的网络犯罪条约,但全球范围内缺乏一部具有普遍约束力的国际公约。这种法律基础的缺失,使得跨国网络犯罪治理中的公私合作陷入混乱。比如,中国与《网络犯罪公约》缔约国的私营部门合作打击网络犯罪时,面临着数据披露及共享准则不清晰的问题。在处理客户敏感信息时,也缺乏明确的指导原则。当区域性条约与国内法律发生冲突时,与国外私营部门的合作变得十分复杂。

从国内法角度看,中国目前主要依赖 2017 年颁布的《网络安全法》。该法虽鼓励公私合作,但重点在于私营组织对公权力的协助义务,而非双方均衡的公私合作治理模式。此外,国际法和国内法的双重不足,导致网络犯罪治理公私合作的法律依据模糊,合作的法律效力薄弱,甚至缺乏约束力,这严重影响了私营部门的合作积极性。2013 年联合国发布的《网络犯罪综合报告》显示,政府正式建立的合作关系多涉及关键基础设施公司,如公用事业和电信公司。其他公私合作关系则多基于法律协议、谅解备忘录或“任务小组”成员资格等非正式机制。以法律作为合作依据的比例极低,仅占 5% 左右。在法律基础薄弱的背景下,网络犯罪治理的公私合作实践面临诸多困难。

2014 年,国际刑警组织在新加坡成立全球创新中心,旨在协助跨国行动。该中心通过建立快速反应机制,确保在跨国网络犯罪事件发生时能够迅速共享信息并协同执法。此外,该中心还定期举行多边或双边会议,促进各国在网络犯罪防范和打击方面的经验交流,尤其是在电子证据的跨境传递和使用方面,明确了各国的权利与义务,避免了因法律冲突导致的执法困难。2024 年 12 月 24 日,联合国大会一致通过具有法律约束力的《联合国打击网络犯罪公约》,旨在加强国际合作,预防和打击网络犯罪。该《公约》是全球网络犯罪治理国际合作的重要成果。作为一项具有里程碑意义的国际法律文件,《公约》不仅规范了各国在网络犯罪领域的立法和执法合作,还将对国际刑事司法合作和跨境执法行动产生深远影响,为全球网络空间的安全与稳定奠定坚实的法律基础。

#### (五) 公私合作侦查与电子数据获取的困难

公私合作在网络犯罪案件侦查和电子数据获取方面也面临着诸多困难。首先，网络犯罪行为的报案率极低，这直接影响了执法机构发现犯罪的能力。据 2023 年 1 至 11 月的数据显示，检察机关共起诉各类网络犯罪 28 万人，同比上升 35.5%，占全部刑事犯罪的 18.8%。报案率低由多种原因造成。一方面，公众对警方处理网络犯罪的能力信心不足，部分受害者甚至未意识到自己已受害，或不清楚如何报案，还有些受害者因感到羞耻和尴尬而不愿报案。这些因素使得执法部门需投入更多资源主动侦查犯罪。另一方面，公私合作中的数据共享面临难题，私营部门因信任缺失而态度消极。企业在未充分评估自身安全漏洞前，公开这些漏洞可能带来巨大风险，如损害公司市值、信誉和客户信任，引发监管和民事责任问题。尽管各国公司法要求对重大风险及时披露，但实际执行效果不佳。此外，私营部门还担忧执法机构接触企业核心机密，使企业面临诸多责任和监管风险。再者，网络服务提供商对数据的存储政策不一，部分信息仅在用户账户活跃时保存。这可能导致公共部门在获批获取数据时，相关电子数据已消失。由于报案率低、缺乏统一的网络犯罪信息共享机制、协调的立法和机构平台，公共部门在侦查和执法中获取电子数据困难重重。

在打击跨国网络犯罪时，获取他国电子数据通常依赖国际司法协助或双边、多边协议。这种方式虽能保障证据所在国的司法主权，但存在程序复杂、效率低的问题。例如，一些执法机构表示从境外网络服务提供商那里获取电子数据的过程相当冗长，且难以确定“电子数据实际所在地既有法定权力又有技术能力的外国当局”。在网络犯罪中，电子数据不稳定、易灭失，需要快速保存和提取，因此这种跨境的正式合作机制在取证效率上的缺陷日益明显。

对此，近来欧美一些国家选择以非正式合作形式直接联系境外网络服务提供商，获取用户、通信或内容数据等直接证据。对于能否允许一国避开国际司法协助和执法合作渠道，直接向外国私营部门调取电子数据，各国看法不一致。支持方大多是《网络犯罪公约》的签约国，其主张应允许国内执法机构直接向境外互联网企业和组织调取证据，且《网络犯罪公约》已将此种途径作为更便捷程序加以规定在其中。反对方则表示，若许可符合欧美执法标准的数据跨境流动，可能会对国家主权和互联网企业数据安全造成危害；跨境取证必须尊重证据所在国主权，不能仅考虑到因国际司法协助和执法合作导致的取证效率低这一问题，而应通过完善司法协助和执法合作的程序和方式以提高取证效率，同时保障相关企业和个人的正当权益。无论是正式合作抑或是非正式合作，跨国网络犯罪治理的公私合作实践往往由于涉及国家主权问题而尤为复杂。当前跨国网络犯罪数量不断增长，如何更好地促进公私部门间的合作，成为国际社会亟待解决的问题。

## （六）跨国网络犯罪治理中的公私合作信任障碍

传统上，政府依赖公力模式来治理犯罪，而私营企业则更关注盈利，忽视了网络安全的长期性和全球性。由于跨国网络犯罪涉及不同国家的法律、政策和文化差异，治理过程中的信任和合作障碍尤为突出。政府部门往往对私营企业的能力和责任心持怀疑态度，认为它们在治理网络犯罪方面缺乏动力和技术支持。此外，许多企业尤其是中小型企业，对网络安全的重视程度不足，认为自己面临的网络攻击风险较小，甚至忽视安全漏洞的存在。这样的观念使得跨国合作变得更加困难。跨国网络犯罪涉及复杂的技术层面和法律问题，各国之间在信息共享、数据保护和法律管辖等方面的差异，增加了跨国合作的难度。以欧洲的 GDPR 为例，其严格的数据保护法规与美国的做法存在冲突，影响了跨境信息共享的效率，阻碍了跨国治理的协作。

2017 年，国际执法机构联合关闭了 AlphaBay 市场，这是全球最大的地下黑市之一，涉及大量跨国网络犯罪，尤其是毒品、武器交易和黑客服务。此次行动由美国、加拿大、泰国、法国等国家的执法机关共同执行，但在实际操作中，跨国合作的难度显而易见。尽管多个国家联合行动，AlphaBay 的创办者

Alexandre Cazes 在泰国被捕后自杀，部分被黑市用户的数据难以追溯，执法部门面临跨境数据共享难题。在这一案件中，跨境合作的最大难点之一是各国执法机关与私营企业之间的信息共享问题。比如，虽然美国 FBI 成功获取了一部分数据，但欧盟和亚洲地区的法律法规在数据跨境传输和隐私保护方面存在严重冲突，影响了跨国调查的进展。同时，许多网络公司在协助政府时也表现出一定的回避态度，担心过度合作可能会损害其客户隐私和商业机密。

跨国网络犯罪治理中的一个核心问题是信任的缺失。信任缺失主要表现在两方面：第一，政府在与私营部门合作时，往往担心其以自身利益为先，难以将公共安全置于首位。第二，私营企业对政府的监管能力和合法性产生疑虑。重大网络犯罪案件中的技术侦查措施是可采且必要的。然而，不当地应用技术侦查措施也将给公民隐私带来极大威胁。因此，在涉及跨国法律适用时，私营企业担心参与合作会招致不必要的法律风险和公众信任危机。两者之间的信任鸿沟导致了公私合作模式的低效和矛盾。此外，跨国网络犯罪的跨国性使得国际司法协作必须仰仗国际法律框架的统一。然而，各国在隐私保护、数据保护和网络安全方面的政策差异，形成了复杂的法律冲突。例如，某些国家的隐私保护法要求不披露特定的用户数据，而其他国家则要求企业配合提供数据，此类冲突严重影响了信息共享的有效性。

### （七）跨国网络犯罪治理中“打击前置化”理念的匮乏

在跨国网络犯罪治理中，传统的“重打击、轻预防”理念依然占据主导地位，轻视了“打击前置化”的重大作用和时代意义。我国以及其他一些国家在跨国网络犯罪治理上偏重事后打击，忽视了预防工作。这种理念的根源在于过于依赖政府主导的“公力模式”，忽视了私营部门在网络安全中的重要角色，尤其是在跨国合作中，预防措施的缺乏成为治理中的重大障碍。网络犯罪的预防需通过多层次的防范机制来降低其发生的风险。这不仅仅依赖政府的监管，还需要私营企业和普通网民的积极参与。然而，跨国治理面临多重挑战。首先，各国的法律框架和数据共享机制不一致，使得跨境合作难以顺畅进行。其次，小型私营企业在资源有限的情况下往往缺乏有效的网络安全防护措施，无法为预防提供支持。

公私合作模式的主要障碍表现在三个方面。第一，信息共享存在困难。跨国网络犯罪治理依赖大数据和信息共享，但各国对数据保护的法规差异使得信息流通受到限制。许多国家缺乏统一的信息共享平台，影响了跨境合作的效率。第二，私营部门参与度不足。部分私营企业，尤其是中小型企业，因成本和资源限制，难以建立有效的网络预防机制。此外，许多企业更加关注短期利润，而非网络安全的长远建设，导致其在公私合作中缺乏积极性。第三，政府主导地位的僵化。在我国及其他一些国家，政府仍主导网络犯罪治理，并对私营部门的能力持怀疑态度。这样的思维模式降低了私营企业的参与意愿，限制了公私合作的效果。

论及跨国合作中的实践问题，研究发现，跨国网络犯罪治理的难度不仅体现在法律协调和信息共享的障碍上，还体现在各国对网络犯罪的不同理解和应对方式之差异上。欧盟和美国之间的“隐私盾”协议（EU-US Privacy Shield）即为典型案例，尽管该协议旨在规范跨境数据传输，但因隐私保护标准差异而受到欧盟法院的挑战，影响了数据的流动和跨国合作。这种法律冲突突显了跨国网络犯罪治理中面临的重大障碍。

## 三、跨国网络犯罪治理公私合作困境之出路

数字社会的特征，一方面表现在跨边界的创新发展与快速融合，另一方面表现在公私边界是法治和自由的基础。数字治理中的公私合作对于数字中国建设具有理论价值和实践意义。因此，对于我国既有的公私合作模式，确有必要厘清治理主体之间的权力边界、责任根据、权利义务和合作路径，共同为促

进我国数字法治建设提供理论依据和经验借鉴。鉴于网络犯罪治理公私合作模式所面临的诸多困难与挑战，为对该模式进行完善，笔者提出以下建议。

### （一）数据主权博弈与跨境管辖权冲突下的合作路径

在数字全球化的时代，跨境数据流动为跨国网络犯罪治理带来了前所未有的挑战。网络犯罪的迅速发展和犯罪主体的跨国性要求各国在国际司法合作中加强协调。然而，数据主权争议和管辖权冲突已然成为跨国打击网络犯罪过程中最为突出的障碍，不仅影响国际司法的高效运作，还极大程度制约了公私合作机制的有效实施。因此，为了有效落实跨国网络犯罪治理中的公私合作模式，解决数据主权和跨境管辖权的冲突问题，笔者将进一步探讨如何通过具体对策，真正让跨国合作和数据治理框架落地，一定程度上确保公私合作的顺利开展。

#### 1. 建立全球统一的数据治理框架

跨国网络犯罪的治理离不开全球统一的数据治理框架。然而，现有的数据保护标准不一和国家立法差异导致了跨境数据流动中的争议与冲突，直接影响了公私合作的实效性。为此，必须推动建构一个具有强制执行力的数据治理框架，以便各国能够在全球数据治理的共同规则下协作。为此，以下措施可供参考。

第一，制定具有法律约束力的国际公约。以现有的跨国合作协议为基础（如《跨太平洋伙伴关系协定》和《数字经济伙伴关系协定》），依据全球公约以统一跨境数据流动的标准。此外，还需通过世界贸易组织（WTO）或联合国制定《全球数据流动协议》，确保所有国家遵循统一的规则与标准，为跨国公私合作提供法律保障。

第二，实现数据主权与数据安全的动态平衡。各国应在全球数据治理规则中，就如何平衡数据主权与隐私保护达成一致，例如在跨境数据请求时设立标准化的“数据保护协议”（DPA）。这一协议将确保数据的合法使用，受到有效保护，避免国家主权与隐私保护之间的冲突，从而为公私合作提供稳定的法律框架。

第三，建立开放透明的跨境数据共享平台。为了提高跨国数据共享的效率和透明度，各国应共同开发遵循统一标准的数据共享平台。该平台能够让各国执法机关按照相同标准和程序处理跨境数据请求，并确保公私合作过程中各方的合规性与透明性。

#### 2. 突破公私合作中的技术障碍

在大数据时代，跨境取证是跨国打击网络犯罪过程中不可忽视的问题，取证请求和流程常常受到管辖权与数据敏感性等因素的影响，而跨国取证机制的灵活性和实操性又直接影响公私合作的流畅度。因此，必须从实际操作层面，推动构建更加灵活和高效的跨境取证机制。

为此，首先可引入动态跨境取证规则框架。依据案件的性质、数据的敏感性及其潜在影响等因素，实施“分级取证”。例如，对于普通网络犯罪案件，采取简化流程；对于涉及国家安全或敏感数据的案件，采用更为严格的审查程序。这一分层取证机制能够根据案件取证难度进行灵活调整，保证数据流动的安全性和合法性，同时减少企业和执法机关的操作负担。其次应统一数据加密与隐私保护标准。随着加密技术的进步，跨境数据传输的安全性和隐私保护愈加重要。国际社会应制定跨境数据加密的国际标准，确保数据在流动过程中不被泄露。这一标准将在协助打击跨国网络犯罪的同时，避免因数据泄露而对个人隐私和企业信息安全造成损害。最后，应建立跨国“取证合作中心”。为确保取证流程的高效性，设立国际化的“跨境取证合作中心”确有必要，且应由国际刑警或联合国等国际组织主导。该机构将协调各国司法机关的数据请求和处理工作，从而简化各国执法系统之间的协调流程，提高跨国合作效率。

#### 3. 完善公私合作机制

跨国网络犯罪治理中的公私合作，其实质是公共部门与私营部门之间的协作。然而，当前的合作模式普遍缺乏充分的法律保障和激励机制，导致企业往往缺乏主动参与的动力。为了克服这一难题，必须在实践中构建更加完善的公私合作机制。

第一，应完善企业法律保障体系。政府应制定明确的法规体系，如制定“网络企业司法合作保障法”，确保私营企业在跨境网络犯罪治理中的地位有法可依，在提供数据时能够得到隐私保护和法律支持，从而减少企业面临的法律风险。第二，需制定跨国数据隐私保护协议。为增强企业在跨国合作中的信任度和积极性，本国政府应鼓励跨国互联网企业与各国政府签订数据隐私保护协议，详细规定数据在跨境流动中的保护要求以及执法机关取证时所必须遵守的操作流程，从而提升企业配合司法调查的意愿。第三，加快建立公私合作激励机制。政府应制定有效的激励方案，例如税收减免、补贴等，以鼓励私营企业加强网络安全建设，积极参与国际合作。通过此类激励措施，不仅有助于企业降低合规成本，还有利于积极推动全球网络犯罪治理。第四，还需设立跨国网络犯罪应急响应小组。为应对突发跨国网络犯罪，公私部门应共同建立跨国网络犯罪应急响应小组。该小组将由政府提供法律保障，企业提供技术支持，以快速响应并打击跨国网络犯罪。

#### 4. 国际法律合作与跨国法律协调

目前国际层面已有多个国际合作框架，但跨境数据请求和统一的取证标准仍未得到有效落实，公私合作的实施受到制约。因此，国际法律合作和跨国法律协调必须实现从理论到实践的转变，对此，可选择以下路径：

第一，为了确保数据请求的统一性，国际社会应制定具有强制约束力的国际协议，要求各国在数据请求和取证方面遵循统一标准，以减少跨境数据流动中的管辖权冲突，为公私合作提供法律保障。第二，专门设立跨国法律协调小组。由联合国或国际刑警等机构牵头建立跨国法律协调小组，定期评估各国数据主权争议和跨境管辖权冲突的解决进展，并推动国际合作和法律框架的持续改进。第三，成立敏感数据的跨国协调机制。早在《云法案》正式出台前，美国实际上已经在根据现行法律向境外调取数据了，而《云法案》相当于赋予了缔约国家调取存储于美国数据的权力。有学者指出，“这归根结底依然是一种国际地缘政治的外化和在数据治理领域的具体实现。”<sup>2022</sup>年，英美两国间已经签署《数据访问协议》（以下简称“《协议》”），该协议将允许两国的执法机构向对方索取用户互联网数据。由此，对于涉及跨境调取敏感数据信息的案件，可将《协议》作为参照样板构建国与国之间数据流动的多边或双边规则，倘若规则规定执法机关有权避开现有法律及法院裁决，直接获取企业所掌握的个人信息，就应高度重视此举是否存在侵犯用户在其他国家数据隐私权利的潜在风险。因此，对于敏感数据的跨境流动，应在全球范围内设立专门的法律框架，规定敏感数据的处理流程，避免数据流动过程中侵犯国家主权或个人隐私。

要真正解决跨境数据流动中的数据主权争议与管辖权冲突，必须通过切实可行的法律与操作机制，涵盖从数据请求、跨境取证到隐私保护、跨国合作的各个方面。通过搭建更加高效的国际合作框架、灵活的跨境取证机制以及切实可行的公私合作模式，跨国打击网络犯罪的障碍将逐步消除，公私合作将迎来新的发展机遇。

## （二）合规困境之出路

跨国网络犯罪治理中的公私合作机制运行和有效落实受制于复杂的法律冲突、数据主权对立和企业合规压力等多个原因。尽管国际合作倡议和国内法律改革如火如荼地进行，但实践中仍面临执行困难，公私合作效果不佳。要真正破除这一困境，必须在深入分析既有措施执行难题的基础上，提出更具可操作性的解决方案，从制度、执行与监督三个层面入手，确保措施不仅能出台，更能真正落地。

### 1. 制度层面：推动国际法律协调，化解法律冲突

《布达佩斯网络犯罪公约》和《数字经济伙伴关系协定》（DEPA）等国际协议的涵盖范围有限，许多国家未签署加入或未充分履行。针对这一问题，应针对性制定全球性数据治理协定，明确数据跨境流动标准、执法合作机制和数据隐私保护责任。例如，可借助 G20、联合国等多边平台，制定具有普遍约束力的《全球跨境数据合作框架协议》，以法律条文形式细化跨境数据请求程序、数据分类标准和争端解决机制。

针对各国高度关注的数据主权敏感性，创新性地设立“数据中立托管平台”，由多国联合监管机构或国际组织（如国际刑警组织、联合国毒品和犯罪问题办公室等）管理。涉案数据由私营企业交由平台托管，执法机构根据透明、统一的规则提出数据调取请求，在平台核查合法性后决定是否授权访问。这一机制避免了企业面临法律冲突导致的两难选择，既尊重数据主权，也满足跨国执法需求。

### 2. 执行层面：健全国内法律与企业合规机制

各国需在刑事司法体系中明确区分公共安全与个人隐私保护，制定统一的数据分类分级规则与跨境流动管理规定。对于涉及国家安全、重大犯罪的数据，建立快速、绿色跨境数据合作通道，简化审批流程；对于一般数据，设置标准化授权机制，确保数据调取程序的合法性和透明性，做到既提升打击犯罪的效率，又保障个人数据安全。

中小企业在合规方面往往显现出其在资源和能力方面的匮乏，在跨境合作中缺乏积极性。政府应根据企业规模和涉案风险，设立分级合规标准：大型跨国公司承担更高的协作义务，如须专门设立跨境数据响应部门；中小企业则只需完成基础配合任务。对合规成本较高的企业，政府可提供税收减免、财政补贴或法律援助，缓解企业负担。行业协会和商会应主导制定行业数据治理和跨境合作指南，明确企业在应对跨国网络犯罪中的责任边界。鼓励企业间建立数据共享和应急响应联盟，降低单个企业独立应对跨境执法请求的法律风险。借助行业自律标准与企业合规联盟，推动行业内部形成合规共识，提升整体响应能力。

### 3. 监督层面：引入动态评估及强化合规问责

建立跨国数据合作透明度报告制度，要求参与跨境数据合作的企业定期发布透明度报告，披露配合执法的数据请求数量、类型和处理结果。此举既增强企业的透明度，消除公众对隐私泄露的担忧，又便于政府监督企业是否履行合作义务。对于拒绝合作或虚假合规的企业，设立法律责任追究机制，强化问责。

此外，应借助第三方独立监督机构强化执法合规性。设立跨国独立监督机构（如国际数据合规委员会），对政府部门和私营企业在跨境数据合作中的合规行为进行监督，确保企业不因政府压力而过度配合，导致用户隐私泄露，或因商业利益拒绝合法执法请求。该机构可接受跨国数据争议投诉，并提出仲裁建议。建立跨国数据合作动态评估和反馈机制，定期评估公私合作执行效果，以便公私双方主体针对执行漏洞和新兴挑战，及时调整合作策略，完善法律规定，确保制度与实践相匹配，避免“有制度无执行”的问题。

要真正破解跨国网络犯罪治理中的企业合规困境，需要多层次、全方位的制度创新和执行保障。从国际合作的法律协调，到国内法规的细化完善，再到企业合规机制的优化与监督，每一环节都要确保闭环管理，避免政策落地后因执行不力而失效。唯有实现多边法律框架、数据托管机制、分级合规义务、行业自律和独立监督的有机结合，才能真正破解合规困境，推动公私合作在跨国网络犯罪治理中有效落地。

## （三）跨国网络犯罪治理政策的理念革新

为有效推动跨国网络犯罪治理政策的理念革新,以保证公私合作模式的高效运行,必须从政策引导、法律保障、合作机制和能力建设等多维度提出切实可行的对策,并确保各项措施具有可操作性和可落地性。

公共部门需要全面转变以打击和控制为主的传统治理思路,积极引导和激励私营企业深度参与跨国网络犯罪治理。在政策层面,政府应通过专门立法明确私营部门在网络安全防护和跨国犯罪打击中的义务和责任。对此,可借助修订或补充《网络安全法》,制定“跨国网络犯罪治理公私合作条例”,细化企业在数据安全、威胁情报共享和协助执法方面的法律责任和操作流程。与此同时,政府应设立激励与惩罚并行的政策机制。例如,针对积极参与跨国网络犯罪治理的企业,提供税收减免、政府采购优先权、品牌信誉认证等正向激励;对拒绝合作或违反安全管理规定的企业,则实施罚款、业务限制甚至暂停网络服务等惩罚措施,形成有效的激励与约束双重机制。

企业自身也需主动强化网络安全能力和风险防控意识。具体而言,应增加对安全技术研发和基础设施建设的投入,建立多层次、全方位的网络安全防护体系。例如,企业需设立专门的网络安全管理部门,配备专业技术人员,持续对网络系统和数据存储设施进行安全审查,并提升全员的安全意识和合规意识。

行业协会和社会组织在推动公私合作中的作用也不容轻视。行业协会应积极制定并推广行业数据安全自律标准和网络安全合规规范,推动企业履行网络安全责任。具体操作上,可通过组织网络安全专题培训、行业安全论坛和跨企信息共享机制,促进企业间、企业与政府间的信息交流和协作。针对重点行业和关键基础设施领域,行业协会还可推动建立行业安全风险监测预警平台,实时共享行业安全动态和威胁情报,增强行业整体网络安全防护能力。

因此,推动跨国网络犯罪治理政策的观念转向,必须形成政府、企业、行业组织和公众多方联动的合作格局。通过政策引导、法律保障、机制创新和能力建设四大举措的联动实施,构建全方位、立体化的跨国网络犯罪治理体系。

#### （四）夯实跨国网络犯罪治理公私合作的法律基础

跨国网络犯罪治理的有效推进,公私合作模式的全面落实与强有力的法律保障密不可分。当前,全球范围内网络犯罪治理的法律框架和操作机制存在一定缺失,国际层面缺乏统一的法律规范,国内层面缺乏系统化的法律制度,这严重制约了公私合作模式的有效实施。因此,为有效推动跨国网络犯罪治理中的公私合作,必须从国际法律框架、国内法律制度和数据合规标准等方面进行全面细化和完善,确保每一项措施具备可操作性并能够落地实施。

加快完善国际法律框架是跨国网络犯罪治理的基础是首要举措。联合国等国际组织需进一步推动《联合国打击网络犯罪公约》的细化和落实,在公约中明确各国政府与私营部门在数据共享、跨境执法协作、信息安全标准和隐私保护方面的具体权利和义务。例如,各国执法机构在跨境数据调取中必须遵循统一的申请和审批程序,明确数据访问的范围、时效和合规要求,避免因操作流程不统一导致执法效率低下和数据主权冲突。公约应设立跨国数据访问机制,规定数据请求方应通过所在国执法机构提交正式请求,并经过多国审核后方可调取数据,从而在保障数据安全的前提下提高执法效率。此外,可借鉴《布达佩斯网络犯罪公约》和《欧盟数据保护通用条例》(GDPR)的经验,将数据安全、隐私保护与执法合作纳入法律框架,确保全球范围内跨国网络犯罪治理在法律制度上的对接和协同。

其次,应建立跨国执法合作平台和争端解决机制。在国际法律框架下,由各国执法机关与私营企业共同参与,成立跨国网络犯罪执法合作平台。平台将设立统一的数据调取和证据共享流程,要求各国在案件侦办中使用统一格式的电子数据请求表,并明确数据使用范围、保密要求和时效期限。该平台还需设置争端解决机制,针对数据主权与隐私保护冲突,授权第三方仲裁机构或专家委员会进行独立裁决,

确保合作高效推进。例如，在数据共享产生争议时，合作各方可通过专家小组快速评估法律冲突并提出解决方案，避免跨国执法合作因法律分歧陷入僵局，造成效率低下。

推动跨境数据共享标准化和安全认证体系也至关重要。各国需联合制定跨境数据共享的标准化流程和安全认证机制，涵盖数据分类分级、脱敏处理和加密传输等关键环节。建立统一的数据分类标准，明确敏感数据、个人隐私数据和一般商业数据的不同管理要求。针对敏感数据，要求跨境传输前必须完成数据脱敏和加密处理，确保数据在传输和使用过程中不被滥用或泄露。各国还应联合推动跨境数据共享安全认证体系，参考 ISO/IEC 27001 等国际标准，认证企业和机构的数据安全管理水平，合规企业方可参与数据共享和执法合作。跨国企业在数据传输和共享时，必须通过安全审查和认证，确保数据流动的合规性和安全性。

在国内法律制度建设方面，可在《网络安全法》的基础上，结合审判和检察机关在办理网络犯罪案件过程中具体应用法律的有关情况，作出相关司法解释，细化公共部门与私营部门在网络犯罪治理中的合作方式和法律责任。法律需明确数据共享、技术支持和信息披露的具体程序，规定私营企业在何种条件下可以合法向执法机关提供用户数据，并要求在数据共享时必须进行脱敏处理和加密传输，以保障用户隐私和数据安全。同时，应明确公共部门在信息使用和管理中的责任，防止滥用数据资源。为进一步推动合作，国家应设立跨部门的网络犯罪治理公私合作协调机构，由公安、司法、网信办和通信管理局等公共部门联合私营企业和行业协会共同组成，推动跨行业、跨部门的常态化合作。该机构还需定期组织跨国联合演练，发布网络安全威胁预警，开展跨国案件联合侦查，并及时更新合作指南和操作规范，确保合作机制高效运作。

为确保数据合规和执法标准化，制定专门的数据合规管理条例尤为重要。条例需明确私营企业在数据收集、存储、处理和共享过程中的法律义务，建立跨境数据流动审批制度，要求企业在进行跨国数据传输前需通过数据安全评估和合规审查。数据传输前，企业需提交详细的数据处理和安全保障计划，接受监管部门审核后方可操作。此外，应推动私营企业与执法机关建立标准化的执法对接流程，统一证据提取、数据共享和案件协作的标准，确保执法活动合法、规范、高效。

在推动企业合规和激励方面，应根据企业规模和业务特点，设置差异化的合规责任。大型互联网企业需承担更多的社会责任，建立高级别的数据安全防护体系，参与跨境数据流动合作项目；中小型企业则根据实际能力承担适度的协作义务，避免合规成本对其经营产生过大负担。政府可通过税收优惠、政策补贴等方式激励企业积极履行合规责任，参与跨国网络犯罪治理。另外，应建立数据安全合规认证体系，对积极参与公私合作、履行合规义务的企业授予认证标识，并纳入企业信誉评价体系，使企业合规表现直接影响市场准入和政府采购资格，形成正向激励机制。最后还应重视推动行业协会和第三方组织在合作中的作用，鼓励行业协会制定行业自律标准，协助政府监管和执法。行业协会可在企业和政府间搭建沟通桥梁，促进信息共享和技术交流，推动行业整体合规水平提升。通过多方协作，形成政府、企业和社会多元参与的跨国网络犯罪治理体系。

## （五）搭建网络信息共享平台

该平台应从法律保障、技术支撑、操作流程、信任机制和跨境合作等方面进行系统性设计和细化，确保平台的实际可操作性和高效运行。

在法律保障层面，为了确保信息共享平台合法合规运作，各国需确立数据共享的法律基础，通过立法为平台的建设和运行提供法律依据。首先，推动制定专门的《跨国网络犯罪信息共享与数据合作条例》，明确规定公共部门和私营企业在数据共享、技术支持和案件协同侦查中的法律责任和义务。条例应细化数据调取的合法程序，明确何种情况下可以启动紧急数据获取，保障共享数据的合法性和安全性。其次，

应建立数据共享的免责机制，明确规定在平台上依法共享的数据不会导致企业承担额外法律责任，从而降低企业配合执法的法律顾虑。对于涉及用户隐私和商业机密的数据共享，必须规定严格的数据脱敏和加密要求，确保在合法合规的前提下高效共享数据。

需确保强有力的技术支撑。信息共享平台的安全性和稳定性是公私合作的核心保障。平台应采用多层加密技术、区块链追踪机制和访问权限控制等技术手段，确保数据在传输、存储和使用过程中的安全性和可追溯性。平台建设需细化数据分类与访问权限机制，将数据分为普通数据、敏感数据和机密数据，不同级别数据由不同级别的用户在授权范围内访问和使用。例如，普通数据可供所有执法机关共享，敏感数据仅限于案件相关人员在加密环境下访问，机密数据则需经过严格审批和多方授权方可使用。为了提高平台的实时性和响应速度，平台应集成智能预警系统和自动化数据分析工具，实时监测潜在的网络威胁和犯罪行为，自动筛选与案件相关的数据，为执法机关提供精准的情报支持。

为了确保数据共享的高效性和规范性，平台需制定详细的操作流程。平台应设立“数据紧急保全机制”，允许执法机构在发现潜在犯罪行为时，向企业发出“数据保全令”，企业需在接到命令后的1小时内冻结相关数据，防止数据被篡改或删除。同时，针对跨国案件，平台应设置“快速取证通道”，简化数据调取申请流程。跨国执法机构可通过平台提交标准化的数据调取请求，平台自动对接私营企业的合规部门，实现数据调取的实时对接与快速反馈。此外，平台应设置“案件协同侦办区”，执法机构和私营企业可在此共享案件相关线索、侦查进展和执法需求，形成实时互动的合作机制。

此外，还需注重跨境合作为网络信息共享平台所增加的效益。为解决跨国数据调取和共享中的法律冲突，应推动国际数据共享标准化，使国际社会制定统一的数据共享规则。各国可在《联合国打击网络犯罪公约》的框架下，签订多边数据合作协议，明确跨境数据调取的法律依据、程序和安全标准。平台应优先在区域性合作组织（如东盟、欧盟、亚太经合组织）中试点推行跨境数据共享机制，积累经验后逐步向全球推广。通过多边合作机制，推动跨国执法机关和私营企业在数据共享、案件协同、证据调取等方面的无缝对接。此外，建立多边争端解决机制，针对数据共享过程中的主权冲突和隐私保护争议，通过专家仲裁、第三方评估等方式高效解决，确保跨境合作的顺利进行。

最后，应确保对平台进行动态评估与持续优化。信息共享平台的建设和运行是一个动态过程，需根据技术发展和网络犯罪形势变化不断调整和优化，才能保障平台长期高效运作。政府和私营企业应共同设立平台运营管理委员会，定期对平台的运行情况进行评估，发现问题及时改进。平台应引入人工智能、大数据分析等先进技术，持续提升数据处理和 Analysis 能力，以适应新型网络犯罪的侦查需求。定期开展公私合作联合演练，检验平台的应急响应和协同作战能力，并根据演练结果完善操作流程和技术细节，确保平台始终保持高效运行状态。

## （六）以对话协商方式提升透明度和信任度

建立稳固公私合作关系的核心在于双方互信。然而，目前公私部门在信息和资源共享方面的表现仍不理想。虽然执法机关通常持有法院批准的电子数据获取令等合法凭据，但私营企业为了保护自身隐私和客户信息，往往对执法机关的非正式请求反应缓慢。要改变这种状况，可从以下几方面着手：

首先，要搭建公私双方的交流与协作桥梁，尤其是在共同维护社会安全的目标下，促进双方合作。考虑到犯罪预防信息的敏感性以及公共部门的权威性，政府应主动与私营企业建立稳定的合作关系。具体来说，可以成立专门机构作为沟通平台，将私营部门在网络安全方面的关切与公共部门的执法需求有效对接。比如，在国际刑警组织与微软等大型科技公司合作时，就发挥了协调侦查任务与电子数据获取工作的纽带作用。

私营企业在与公共部门建立合作时，亦应明确自身需求和利益诉求，以便在合作过程中灵活调整合

作机制，确保合作关系的长期稳定。这种基于利益对等的明确沟通，有助于增强合作的实效性和持续性。此外，政府也应通过财政支持和激励政策鼓励私营部门积极参与网络安全防护。考虑到私营企业在网络安全建设方面投入巨大，公共部门可以提供资金援助、专业培训和技术支持，降低企业防护成本，增强合作意愿。对于已遭受网络犯罪侵害的企业，政府应将其视为受害方，提供政策扶持和资源帮助，以此改善公私部门间的合作氛围，促进信任关系的建立。

### （七）强化跨国网络犯罪预防中的公私合作

为切实推动跨国网络犯罪治理中“打击前置化”理念的落实，必须围绕公私合作模式提出具有可操作性和落地性的具体措施，涵盖信息共享、法律保障、技术防护和公众参与等多个维度。

为有效预防跨国网络犯罪，确有必要搭建一个跨国网络安全信息共享与预警平台，实现公私部门在信息共享和风险预警方面的无缝对接。该平台应采用分层次数据共享机制，将数据根据敏感程度划分等级（如公共信息、敏感信息、机密信息），并根据合作方的资质和合作级别授权访问权限。平台可运用区块链技术，保障数据共享过程的可追溯与透明，避免数据遭到篡改或不当使用。在技术层面，应融合人工智能与大数据分析，实现对全球网络威胁情报的实时监控、解析和警报。提前锁定潜在威胁。例如，平台可以每日自动生成威胁报告，推送给合作成员，涵盖恶意软件传播趋势、网络攻击热点等。为了促进私营部门积极参与信息共享，政府可以设立网络安全信息共享激励机制。参与信息共享的企业，可享受税收减免、优先获取政府采购项目、获得网络安全认证等政策支持。同时，为消除企业对数据泄露和法律风险的顾虑，政府需出台法律豁免条款，规定在合规框架下配合数据共享的企业不承担由此产生的法律责任。

在法律保障层面，各国需推动签订统一的跨境数据共享与执法合作协议。该协议需细化数据调取的流程和标准，明确私营企业在配合执法中享有的权利和义务。例如，跨国数据调取需明确哪些类型的数据可以共享、数据调取请求的提交方式、审批程序和数据加密传输标准，保障数据调取的合规性与安全性。同时，各国国内应出台《跨国网络犯罪防控公私合作条例》，明确数据共享、漏洞披露、网络安全防护等方面的具体要求，厘清公私部门在跨国网络犯罪防控中的职责边界。此外，各国还需设立跨部门网络安全合作协调机制，由公安、网信、司法等政府部门联合私营企业和行业协会共同参与，定期更新合作指南和数据共享标准。针对跨国合作中可能涉及的数据主权和隐私保护问题，法律中应明确企业在跨境数据传输中的法律责任和免责条件，避免因法律空白导致合作停滞。

针对跨国网络犯罪的动态性和复杂性，政府和私营部门需联合开展跨境网络安全预防演练。每年至少组织两次跨国联合演练，模拟多种复杂场景（如大规模勒索软件攻击、跨境电信诈骗、供应链攻击等），通过实战测试各方应急响应能力和协作流程。演练中应细化各方责任分工。例如，政府负责跨国协调和执法响应，私营企业负责技术支持和数据溯源，行业协会提供风险评估和安全建议。演练结束后，需形成详细报告，针对发现的问题制定整改计划，持续改进跨国协作机制。

中小企业通常是网络安全防护的薄弱环节。为弥补这一短板，政府应设立专门的中小企业网络安全支持基金，资助企业进行安全基础设施升级和防护技术研发。大型互联网企业和安全公司也应承担社会责任，向中小企业免费提供基础防护工具和安全咨询服务。政府还应定期发布《中小企业网络安全合规指南》，提供操作性强的网络安全管理规范以供参考，指导企业建立风险评估、漏洞修复和应急响应机制。此外，可以建立中小企业安全支持平台，为企业提供实时的安全漏洞通报和技术咨询服务，如企业可通过平台提交安全事件报告，政府安全机构可即时提供应急响应建议，避免因反应滞后导致重大安全事件。

社会公众亦是预防网络犯罪的重要防线。政府与私营企业应携手推进网络安全教育的普及工作，专

门开设网络安全教育课程。例如，相关教育部门可组织开展线上网络安全教育活动，邀请专业人士讲解防范电信诈骗、保护个人信息等知识，增强师生的网络安全意识。企业可以借助社交媒体、短视频平台等新媒体渠道，积极开展网络安全公益宣传活动，向公众传授防范诈骗、防止数据泄露等基本知识。此外，还应建立匿名举报平台，对于提供案件关键线索的举报者给予荣誉表彰和物质奖励。相关部门还可利用各类新媒体平台广泛宣传网络安全工作成果，引导网络运营者提升安全防护意识，共同筑牢网络安全防线。

面对突发网络安全事件，各国应签署跨国应急联动协议，设立跨国网络安全应急响应中心。该中心需明确各国在突发事件中的信息通报机制、数据共享渠道和责任划分。可设立跨国绿色通道，在紧急情况下允许执法机构绕过常规流程，快速调取关键数据。同时，成立跨国网络犯罪联合调查小组，整合各国执法机构和私营企业资源，提升快速反应能力。例如，当某国发现涉及多国的网络攻击时，可立即通过应急中心通报各方，启动联合调查和追踪行动，最大程度降低损失。

综上，通过构建信息共享与预警平台、完善法律保障、联合开展防护演练、扶持中小企业、提升公众意识和建立跨国应急响应机制，可以系统性地强化跨国网络犯罪的预防与治理。这些细化且可落地的措施，能够有效打破“重打击、轻预防”的传统思维模式，推动“打击前置化”理念的真正落实，形成以公私合作为核心的跨国网络安全防护体系。

## 四、结论

全球数字化进程不断加快，跨国网络犯罪日益猖獗，各国面临重大网络安全挑战。为有效打击和防范此类犯罪，必须打破传统以公权力为主导的治理模式，推动公共部门与私营部门的深度合作。本文围绕跨国网络犯罪治理中的公私合作模式，系统分析了当前存在的数据主权争议、跨境管辖冲突、法律制度不健全、信任缺失以及“重打击、轻预防”观念等影响公私合作机制有效运行的主要障碍，并提出了具有可行性的相应对策。

为破解治理困境，需推动构建全球统一的数据治理框架，完善跨境数据共享与取证机制，搭建高效的跨国信息共享平台，强化法律制度保障并落实企业合规要求。同时，通过多方对话与协商，增强公私部门互信，推动“打击前置化”理念的落实，实现多元主体协同治理。唯有全面整合各方优势及资源，形成高效、公正、透明的合作机制，才能有效提升跨国网络犯罪治理能力与治理效能，切实维护网络空间长治久安，促进全球数字治理体系健康发展。

## 致谢

感谢北京外国语大学法学院提供的学术平台与学习环境。在论文写作过程中，我也受益于学院诸位老师的悉心指导与宝贵建议，在此一并致以诚挚的谢意。

## 参考文献

- [1] Brill Alan. The Need for Public-Private Information Sharing in Cybersecurity[J]. NATO Science for Peace and Security Series - E: Human and Societal Dynamics, 2019, 141.
- [2] Raphael Bossong, Ben Wagner. A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU[J]. Crime, Law and Social Change, 2017, 67 (3).
- [3] S. Boes, E.R. Leukfeldt. Fighting Cybercrime: A Joint Effort[J]. Springer International Publishing, 2017, 185.
- [4] Kristen E. Eichensehr, Public-Private Cybersecurity[J]. Texas Law Review, 2017, 467.
- [5] 郭晶. 网络犯罪侦查——公私合作与权利保护[M]. 知识产权出版社, 2018: 152.
- [6] Roy Hadley. Cybersecurity for Public-Private Partnerships[J]. Security Magazine, 2019 (October).

- [7] 胡铭, 张传玺. 大数据时代侦查权的扩张与规制[J]. 法学论坛, 2021, 36 (03): 5-14.
- [8] 黄风, 赵林娜. 国际刑事司法合作: 研究与文献[M]. 中国政法大学出版社, 2009: 232-241.
- [9] 江溯. 论网络犯罪治理的公私合作模式[J]. 政治与法律, 2020 (08): 38-52.
- [10] 敬力嘉. 网络暴力公私合作治理模式的反思与调试[J]. 江汉论坛, 2023 (05): 136-144.
- [11] Nir Kshetri. India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership[J]. IEEE Security & Privacy, 2015, 13 (3).
- [12] 黎晓露. 网络犯罪侦查公私合作的兴起及其法律规制[J]. 犯罪研究, 2024 (04): 51-62.
- [13] 李彦. 打击跨国网络犯罪国际法问题研究[M]. 中国法制出版社, 2021: 19-37.
- [14] Max Manley. Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership[J]. Journal of Strategic Security, 2015, 8 (3Suppl).
- [15] Aidan McCauley. How to Close Cybersecurity's Widening Workforce Gap: How Are Public-Private Partnerships Helping Solve the Cybersecurity Skills gap?[J]. Security Magazine, 2019 (December).
- [16] Reeder Joe R., Barnsby Robert E.. A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership[J]. The Cyber Defense Review, 2020, 5 (3).
- [17] 裴炜. 网络犯罪治理国际协作: 机制、主题与展望[J]. 中国信息安全, 2020 (09): 81-85.
- [18] 裴炜. 跨境打击网络犯罪中的公私合作[J]. 信息安全与通信保密, 2021 (07): 37-45.
- [19] 裴炜. 论网络犯罪跨境数据取证中的执法管辖权[J]. 比较法研究, 2021 (06): 30-45.
- [20] 裴炜. 网络犯罪治理中公私合作的障碍及其化解[J]. 北京航空航天大学学报(社会科学版), 2021, 34 (05): 33-34.
- [21] 裴炜. 向网络信息业者取证: 跨境数据侦查新模式的源起、障碍与建构[J]. 河北法学, 2021, 39(04): 56-81.
- [22] 裴炜. 刑事跨境取证中的数据安全风险及其应对[J]. 国家检察官学院学报, 2021, 29 (06): 37-54.
- [23] 裴炜. 刑事诉讼中的个人信息保护探讨——基于公民信息保护整体框架[J]. 人民检察, 2021 (14): 6-10.
- [24] 裴炜. 论刑事诉讼中网络信息业者的数据提供义务[J]. 上海政法学院学报(法治论丛), 2022, 37 (06): 60-75.
- [25] 裴炜. 网络空间刑事司法域外管辖权的数字化转型[J]. 法学杂志, 2022, 43 (04): 109-128.
- [26] 裴炜. 刑事数字合规困境: 类型化及成因探析[J]. 东方法学, 2022 (02): 159-173.
- [27] 王文华. 新型犯罪治理与刑法现代化研究[M]. 人民出版社, 2021: 330-333.
- [28] 魏光禧, 刘想树. 跨境数据取证中的公私合作——以《联合国打击网络犯罪公约》为视角[J]. 河北法学, 2024, 42 (08): 78-100.
- [29] 魏光禧, 刘想树. 跨境数据取证中公私合作的具体路径[J]. 中国人民公安大学学报(社会科学版), 2024, 40 (01): 63-74.
- [30] 谢登科. 论技术侦查中的隐私权保护[J]. 法学论坛, 2016, 31 (03): 32-40.
- [31] 熊亚文. 网络金融犯罪的公私合作治理[J]. 南京大学学报(哲学·人文科学·社会科学), 2023, 60 (06): 138-146+160.
- [32] 杨学敏, 刘特, 郑跃平. 数字治理领域公私协作研究述评: 实践、议题与展望[J]. 公共管理与政策评论, 2020, 9(05): 3-18.
- [33] 赵永琛. 《联合国打击网络犯罪公约》的制定问题研究[J]. 武大国际法评论, 2022, 6 (05): 1-20.