

犯罪经济学视角下网络犯罪的深层成因与预防策略研究

● 刘华超



[摘要] 随着信息技术的发展,互联网已经深深地影响和改变了人们的生产生活方式。然而,网络空间的开放性也为各类犯罪提供了滋生蔓延的温床。各种网络诈骗、恶意病毒软件等网络犯罪手段的出现,危害了广大网民的财产安全和生命健康。网络犯罪之所以难以有效遏制,关键在于这类犯罪具有高收益、低成本的显著特征。高匿名性使犯罪者难以被识别和追踪;丰富的网络资源又为犯罪分子提供了各种非法牟利的机会。因此,迫切需要深入剖析网络犯罪的深层原因,以期找到解决网络犯罪扩散的有效途径。本文拟运用犯罪经济学的相关理论,剖析当前网络犯罪增多的经济学原因,并制定切实可行的网络犯罪遏制策略,维护网络环境的安全。

[关键词] 犯罪经济学;网络犯罪;深层成因;预防策略

从犯罪经济学视角下,对网络犯罪的深层成因与预防策略进行研究具有重要意义。随着技术的快速发展,网络犯罪日益复杂,经济利益驱动成为犯罪行为主因。深入剖析其背后的动机与社会因素,有助于制定更有效的预防措施,维护网络空间的安全与稳定。

Q 网络犯罪的概念与特征

(一)网络犯罪的定义

网络犯罪是指在计算机网络或其他信息网络上进行的违法犯罪活动。这一犯罪形式充分利用了互联网的开放性、虚拟性和跨国性等特征,通过网络渠道实施传统犯罪,同时也催生了一系列新的犯罪形式。黑客入侵、病毒传播、网络诈骗、网络赌博、网络侵权等构成了网络犯罪的多个层面。黑客入侵涉及非法侵入他人计算机系统,获取敏感信息或者进行恶意操控。病毒传播通过网络媒介传播恶意软件,对用户设备和数据造成危害。网络诈骗则通过虚假信息获取个人或财产信息,导致经济损失。网络赌博和网络侵权等行为也在网络犯罪的范畴之内。这些行为严重威胁网络安全,侵害他人的合法权益,危及社会公共利益。

(二)网络犯罪的类型和表现形式

网络犯罪呈现多样性,可分为入侵型、破坏型、欺诈型、盗版型等不同类型。黑客入侵涉及非法进入他人计算机系统,擅自掌控或获取数据。病毒、木马程序则通过网

络传播,对计算机数据实施破坏。网络诈骗通过钓鱼网站进行,伪装合法实体,盗取银行账户及游戏账号。网络赌博和色情信息通过网络传播,带来社会不良影响。盗版行为通过网络传播和销售,损害知识产权。综合来看,这些行为破坏了网络安全,影响了个人及社会的合法权益,体现了对网络犯罪的全方位防范和打击的迫切性。

(三)网络犯罪的特征和影响

网络犯罪呈现出显著的特征,包括隐蔽性高、传播速度快、范围广泛、具有较强的跨国性。这种犯罪形式对网络安全构成严重威胁,侵犯知识产权、损害商业利益和个人财产,扰乱网络秩序,导致人们对网络的信任度下降,产生了一系列负面社会影响。网络犯罪的隐蔽性使其在网络空间中难以察觉,而其传播速度较快使其迅速波及全球范围。侵害知识产权不仅削弱了创新力,还直接影响了商业利益和个人财产。网络犯罪不仅是一场技术斗争,更是对网络秩序和社会信任的深刻冲击,其负面影响不断扩大。

Q 犯罪经济学视角下网络犯罪的深层成因

(一)经济利益驱动

网络犯罪的一个主要推动力是经济利益的诱惑。一些黑客以窃取他人计算机系统敏感信息获取不义之财,通过制作并传播病毒实施勒索,或者运营网络赌博和色情网站牟取高额利润。同时,盗版网络作品也成为获取经济收益

的手段。这种利益导向使得一些人不惜违法犯罪，以获取经济回报。网络犯罪的成本较低和获利容易也是其激增的原因。在网络空间中，犯罪者可以匿名行事，利用各种工具和技术实施攻击，使得犯罪的风险和成本相对较低，从而进一步助长了这类犯罪活动的蔓延。犯罪经济学理论强调，当潜在的经济收益大于预期的成本和风险时，就会产生犯罪动机。

（二）匿名性和隐蔽性

互联网的崛起为社会带来了较大的变革，同时也成了犯罪分子的理想场所，其中匿名性是网络犯罪的一个显著特征。在这个数字化时代，互联网为个体提供了一定程度的匿名性，使得执行犯罪活动的个体更容易隐藏其真实身份。通过遮蔽IP地址、使用虚拟专用网络（VPN）等方式，犯罪分子能够在网络空间中操作而不留下易于追踪的痕迹。加密技术和匿名网络工具更是进一步加强了这种隐蔽性。先进的加密方法不仅能够保护通信内容的机密性，还能有效掩盖犯罪分子的身份。匿名网络如Tor(The Onion Router)更是为犯罪分子提供了一层额外的遮掩，通过多层加密和反向传输，使得追踪和识别犯罪分子变得较为困难。这种隐蔽性直接导致法律机构在打击网络犯罪方面面临挑战。传统的调查手段和法律程序通常无法有效适应互联网环境的复杂性。犯罪分子能够迅速地变换身份，使用新的匿名账户和虚构身份，使得追踪的过程变得复杂和漫长。

（三）法律制度不完善

各国在网络领域的相关法规和处罚力度还比较薄弱，这在一定程度上促进了网络犯罪活动的存在和发展。由于网络犯罪存在跨国性特点，不同国家和地区的法律制度难以有效衔接，使得此类犯罪的联合调查和跨国证据固定均面临法律障碍。此外，网络技术迭代更新较为迅速，而法律制度和执法手段跟不上网络空间技术形态的快速演变，这也给网络犯罪留下了可乘之机。因此，完善网络法律法规，使违法成本大幅提高，是遏制网络犯罪的有效手段之一。

（四）技术发展不平衡

当前网络空间面临较大挑战，存在大量系统和软硬件漏洞以及代码缺陷，这些薄弱环节为有犯罪动机的黑客提供了便利通道，使其能够轻松地进行违法活动。网络安全的脆弱性给予了攻击者机会，如果网络技术的防御能力无法跟上攻击手段的更新换代，网络犯罪将如同病毒一样不断“变异”，制造更多的攻击突破点。尤其是最新型的勒索软件和攻击手段不断出现，使网络犯罪的可能性进一步增加。这些先进的攻击工具不仅能够有效地规范网络空间，还能够更具隐蔽性，使得防范起来更为困难。

（五）全球性和跨国性

互联网的全球性为犯罪分子提供了场所，使得网络犯罪

得以超越国界进行。在这个数字化时代，犯罪分子可以通过勒索软件、网络欺诈等手段，轻松地对来自世界各地的目标发动攻击，无需实际出现在被攻击对象所在的国家或地区。这种全球性特征，为网络犯罪提供了便利。网络犯罪的全球性意味着犯罪分子可以选择目标，不受国界和法律的限制。他们可以在各国之间迅速切换服务器，使用匿名的支付方式，使得犯罪活动更加难以追踪和打击。这种全球性特征加剧了犯罪行为的复杂性，使得传统的执法手段难以适应这种新型的威胁。网络犯罪的规模和影响也因其全球性而急剧扩大。一次网络攻击可能同时波及多个国家，影响数以千计的个人、企业和机构。

Q 犯罪经济学视角下网络犯罪的预防策略

（一）加强法律制度建设

第一，加快网络安全法、数据安全法等重要法律法规的立改废工作，以形成一个系统完备的网络空间治理法律体系。这需要及时修订和更新法规，以紧密关注互联网发展的新趋势和挑战，确保法律框架能够有效应对新型网络犯罪的威胁。第二，加大网络违法犯罪行为的立法力度，扩大法律适用范围，加大违法成本。通过明确刑事和行政责任，使网络犯罪分子付出更为沉重的代价，提高法律威慑力。第三，简化立法程序，推动网络犯罪立法快速响应，使之紧跟网络犯罪新动向和新特点。建议采用灵活的立法机制，以便及时应对新型网络犯罪的威胁，保持法规的敏捷性和适应性。第四，加强法治宣传教育，增强全民法治意识，让人们充分认识网络犯罪的危害性，自觉遵纪守法。通过广泛开展法治教育活动，提高公众对于网络法规的了解和认同，形成全社会共同维护网络法治的氛围。第五，完善法律责任追究制度，实行网络实名制，强化法律效果。建议加强对于网络犯罪的定责追究，通过实行实名制度，有效监管网络行为，减少匿名行为可能引发的违法风险，提高网络环境的整体安全水平。

（二）增强网络安全意识

第一，必须加大网络安全宣传力度，通过多种渠道和多样化的形式进行广泛宣传。通过社交媒体、电视、广播等传媒，以及线下活动、宣传册等方式，普及网络犯罪手段的认知，提高公众对于网络威胁的警觉性。第二，建议开设网络安全公众课堂，定期组织培训讲座，传播网络安全知识，教大家具备实际的安全技能。这有助于培养人们对于如何辨别和防范网络欺诈的能力，提高应对网络风险的自我保护能力。第三，建立网络安全志愿服务队伍，动员企业和社会各界力量参与网络安全宣传。通过组织志愿者，可以更广泛地传播网络安全理念，增强社会层面的网络安全意识，形成全社会共同参与网络安全建设的良好氛围。第

四,应从小抓起,将网络安全意识培育融入教育体系。通过在学校设置网络安全教育课程,培养学生对于网络风险的认知和防范能力,从而形成更为健康的网络使用习惯。第五,鼓励技术企业加大网络安全产品研发力度,不断提高产品防护能力。主管部门可以通过激励措施,推动企业研发更为安全可靠的软硬件产品,以提供更强大的网络安全保障,降低用户面临网络威胁的风险。

(三)建立完善的监管机制

第一,必须明确监管部门及其职责,确保监管内容全面无遗漏。通过建立清晰的监管体系,实现对网络空间的全面监管,避免出现监管盲区。这需要制定详细的法规和政策,确保监管工作的有效执行。第二,建立跨部门、跨地区的监管协作机制,实现信息的集中和共享。监管机构应通过定期的协作会议和信息交流平台,加强对网络犯罪情报的收集、分析和共享,以形成更加协同一致地打击网络犯罪的力量。第三,充分利用大数据和人工智能技术手段,以提高对网络异常情况的监测和判断能力。通过数据分析和人工智能算法,监管部门可以更准确地识别潜在的网络威胁,加强对网络犯罪的及时防范和打击。第四,建立网络实名登记制度,对网民的网上活动进行必要的跟踪。这有助于确保网络环境的透明度,减少匿名行为带来的风险,并能够更有效地追踪和处理涉及犯罪行为的网络活动。第五,强调网络服务提供企业的责任,建立上网记录存取制度。监管部门应推动网络服务提供商履行社会责任,确保其保存用户上网记录,以便在必要时进行调查和追溯。第六,要加大对违法网站和信息的管制力度,及时制止其扩散。通过加强对网络内容的审核和监管,能够有效遏制非法信息的传播,保护公共利益和网络安全。

(四)加强国际合作与交流

第一,我国应积极签署相关国际公约,以建立起打击网络犯罪的坚实国际法律框架。这有助于强化国际合作,加大对网络犯罪的惩治力度。第二,通过与其他国家开展联合执法行动,可有效整合全球资源,形成合力,加强网络犯

罪情报交流与跨境追捕,防范犯罪分子逃逸。第三,各国之间应加强网络监测方法与安全防护技术的共享,提升跨国网络环境治理能力。通过合作研发先进技术,共同抵挡网络攻击,确保网络空间的安全。同时,建立合作机制,促进国际社会分享最佳实践,共同努力维护网络生态的整体健康。第四,应加大力度打击利用跨境服务器进行犯罪活动的“跳板”行为。通过国际协作,共同追踪和惩治那些试图逃避国内法律制裁的犯罪分子,确保他们无法在虚拟空间中找到庇护。第五,建立网络安全国际论坛是加强国际合作的关键一环。在这个论坛上,各国可以分享网络犯罪治理理念、政策法规等方面的经验与见解,共同推动全球网络治理体系的不断完善与创新。

Q 结束语

犯罪经济学视角下对网络犯罪深层成因与预防策略的研究,强调理解犯罪动机、经济利益及社会背景的重要性。未来,需要不断深化对犯罪经济学的理解,结合科技创新制定新型防范策略。在这个过程中国际合作将成为关键,需要共同构建跨境打击网络犯罪机制。同时,需要通过法律法规的完善和社会意识的增强,加强对网络犯罪的防控。未来,期待能够构建更加智能、协同、全球化的网络安全体系,确保数字社会的持续健康发展。

参考文献

- [1]王文轩.计算机网络犯罪的国际化新动向[J].网络安全技术与应用,2024(01):125-127.
- [2]梅正崇.我国网络犯罪刑法规制问题研究[J].法制博览,2023(36):115-117.
- [3]姜子明,徐世博.网络犯罪辅助行为的性质[J].中国检察官,2023(24):66-68.

作者简介:

刘华超(1984—),男,汉族,广西南宁人,硕士,湖南天汇湘海咨询管理有限公司,研究方向:刑法。