网络犯罪现场勘查的难点及解决对策

任骋宇

(西北政法大学, 陕西省西安市, 710122; 13708998213@163.com)

摘要:近年来,网络犯罪作为一种新型、频发的高科技犯罪,改变了传统的犯罪形态。其网络环境复杂、多变的特点决定了网络犯罪现场勘查与传统刑事案件现场勘查存在着极大的差异,这对勘查人员提出了新的要求。本文将围绕网络犯罪现场的确认、开展现场保护、现场访问、现场勘验检查、现场分析以及电子数据的收集与固定等方面存在的诸多重难点问题进行分析,结合前沿技术与实际案例,提出具有针对性、可操作性的解决对策,以有效提高勘查人员网络犯罪现场勘查水平。

关键词:网络犯罪现场勘查;难点;对策

引言

随着信息技术的飞速发展,网络空间已成为现代社会不可或缺的一部分。然而,网络空间的开放性、匿名性和跨地域性也为犯罪分子提供了新的犯罪手段,网络犯罪日益猖獗,给社会稳定和人民财产安全带来了严重威胁。网络犯罪现场勘查作为打击网络犯罪的关键环节,面临着诸多挑战。网络犯罪与传统刑事案件相比,犯罪方式和犯罪手段更加隐蔽化、智能化。现场勘查人员在应对以网络化、虚拟化为特点的网络犯罪现场的勘查中面临着诸多难点。而网络犯罪现场勘查是开展网络犯罪案件刑事侦查工作的基础,直接关系到后续侦查工作的开展以及诉讼程序的进行。当前亟待采取一系列对策以提高网络犯罪现场勘查的整体水平,深入探讨网络犯罪现场勘查的难点及解决对策,提高勘查人员勘查能力和水平,为打击网络犯罪以及维护网络安全和社会稳定提供有效的参考和借鉴。

1. 网络犯罪现场勘查概述

1.1. 网络犯罪现场

1.1.1. 网络犯罪现场的概念

在传统刑事案件的现场勘查中,“犯罪现场”[1]这一概念的界定是基于物理空间层面讨论的,在传统视角下,犯罪现场指的是发生犯罪事件的地点和存在与犯罪有关的物品、痕迹、尸体、信息的相关场所。而“网络犯罪现场”不仅包括传统犯罪现场的物理空间,还包括网络犯罪行为发生或呈现结果的虚拟环境,例如服务器、网络设备、协议及用户数据等。网络犯罪现场是指网络犯罪行为发生或结果呈现的具体网络空间及其相关环境,是犯罪分子在网络空间中进行攻击、破坏、窃取信息等非法活动的场所。

1.1.2. 网络犯罪现场的特点

首先,网络犯罪现场具有传统犯罪现场阶段性、特定性、易变性的特点。但区别于传统犯罪现场的暴露性,网络犯罪现场更多呈现的是其隐蔽性、虚拟性、高技术性、电子数据脆弱性的特点。具体而言,网络犯罪的犯罪现场具有高度的虚拟性。犯罪行为通过网络连接进行,以数字化的形式完成,犯罪行为地与结果地往往不是同一个地点,这使得网络犯罪打破了传统犯罪所受地域空间、距离的限制,犯罪现场也因此变得无形和难以捉摸。这种虚拟性使得网络犯罪的侦查和取证工作变得异常复杂,需要借助如区块链电子数据存证技术等专业的网络技术和工具来定位和固定证据,确保数据的原始性和可追溯性。其次,由于网络空间的高度虚拟性,网络犯罪现场具有极强的隐蔽性。犯罪行为在网络上往往体现为某一IP地址和账号,但犯罪分子可以通过伪造身份、使用代理服务器、隐藏IP地址、注册多个账号甚至盗用他人账号的方式进行犯罪,以此来掩盖自己的真实身份和行踪,使得侦查工作更加困难。此外,网络犯罪现场具有高技术性的特点。网络犯罪分子大多精通计算机技术,网络犯罪现场往往涉及复杂的网络技术和计算机元件等,其高技术性大大增加

了网络犯罪现场的勘查难度。在实践中，犯罪分子在针对金融行业的网络攻击中往往能够利用高级持续性威胁（APT）技术，长期潜伏在目标系统中窃取敏感数据，这使得勘查人员需要具备深厚的网络安全技术知识才能有效应对。最后，网络犯罪现场的证据主要以电子数据形式存在，这些证据具有易失性和脆弱性。勘查人员需要进行合理的现场保护并在电子数据证据的提取过程中保护电子数据的原始状态、完整性、真实性。

1.2. 网络犯罪现场勘查

1.2.1. 网络犯罪现场勘查的对象

网络犯罪现场勘查的对象主要围绕计算机网络系统及其相关环境展开，旨在收集和分析与犯罪活动相关的电子数据、物理设备和人员信息。在将网络犯罪现场划分为本地现场及远程现场的研究视角下[2]，网络犯罪现场勘查的对象也可以分为本地现场及远程现场两个部分进行论述。在本地现场中，网络犯罪现场勘查的对象包括犯罪嫌疑人实施网络犯罪活动的物理空间地点、涉及网络犯罪的计算机系统及其附属设备、现场可能存有的痕迹物证、可能存有案件线索或证据的电子数据载体介质、涉案人员等。在远程现场中，其研究对象主要包括计算机系统与附属设备中的电子数据、有计算机数据信息保留的网络传输节点、通讯记录、金融交易记录、计算机的系统设备或应用软件的参数、属性等。

1.2.2. 网络犯罪现场勘查的要点

网络犯罪现场勘查的要点主要在于有效进行网络犯罪现场的确定、现场保护的开展、现场访问的组织、勘验检查的进行、证据的收集与固定、现场分析的展开等勘查工作。网络犯罪现场的确定是网络犯罪现场勘查的起点，对于现场的确定是开展后续勘验检查工作的基础。现场保护是证据原始性、完整性的重要保障，为现场勘查工作提供必要的操作环境，保障现场勘查工作顺利进行。现场访问是侦查人员获取案件基本情况的重要途径，是推动查明犯罪事实、查缉犯罪嫌疑人工作开展的重要环节。勘验检查与证据的收集与固定是网络犯罪现场勘查的最重要的环节之一，是网络犯罪现场勘查工作的核心，为现场访问、现场分析提供有力依据，为确定案件性质、查明犯罪事实及其后续诉讼程序提供重要支撑。现场分析是将网络犯罪现场勘查所获取的线索、证据等信息进行进一步的梳理、判断与分析，回溯案件真实情况，确定后续侦查方向，推动后续侦查工作的顺利开展。

2. 网络犯罪现场勘查的难点

2.1. 网络犯罪现场难以确定

在网络犯罪中，犯罪事实并不像传统犯罪那样易被发现和确定，网络犯罪往往隐蔽而多变。网络犯罪中的犯罪嫌疑人往往作案在某一个地点，犯罪行为却出现在多个不同的犯罪现场，犯罪结果同样出现在另一个地点或其他多个地点。加之网络犯罪中的犯罪嫌疑人会不定期更换作案地点，链接不同的VPN，这就导致网络犯罪的犯罪现场不同于传统刑事案件中处于稳定时空的犯罪现场，网络犯罪现场隐蔽而多变，难以发现和确定。

此外，本地现场的确定在网络犯罪现场勘查中也具有其特殊性，同样不能忽视。本地现场通常指的是可控的、可进入的、可操作的本地现场环境。在网络犯罪中，本地现场主要有两类需要格外注意。一类是犯罪嫌疑人使用过的计算机系统以及该系统所在的物理空间。另一类则是被犯罪嫌疑人攻击或破坏的计算机系统以及该系统所在的物理空间[3]。

2.2. 现场保护困难

现场保护是现场勘查的基础，关系着现场勘查的质量及成败。在网络犯罪现场勘查中，核心的问题在于技术性保护要求较高。网络犯罪现场保护与传统犯罪现场保护不同的核心就在于其需要较强的技术性保护，由于电子数据、电子介质的易失性以及网络系统的虚拟性、易破坏性，勘查人员需要保护电子数据的原始状态及其完整性，因此，如何保证网络犯罪现场中相关计算机设备处于相对独立、隔离的原始状态是一大难题。这要求现场保护人员能够及时判断现场是否有继续进行的安全威胁及扩大损害的可能，并采取正确的应急处置方法。现场保护人员需要具备较高的计算机专业知识和技术水平以便于他们能够迅速识别并保护关键电子数据和电子介质，同时应对各种可能出现的网络攻击和破坏行为。若现场保护人员未能及时发现并阻止黑客的二次攻击、未能及时隔离计算机设备使得电源异常断开，导致部分关键电子数据被篡改、删除或丢失，会严重影响案件的侦查和取证。

2.3. 现场访问要求高

现场访问需要勘查人员根据现场情况随机应变，根据特定犯罪现场制定不同的访问策略，采取适宜的方式方法访问被害人，避免被害人因夸大、隐瞒事实误导侦查人员的勘查方向。同时避免因被害人的配合程度较低而使部分证据无法通过访问查证其真实性、影响到案件完整证据链条的构建的问题的出现。其次，网络犯罪内部人员情况复杂，全面调查计算机网络系统工作人员难度较高，这就要求勘查人员在全面了解涉案人员情况的同时还需要确定重点访问人员，对可能涉及多个部门和层级的涉案人员深入了解其人员分工、访问权限、操作日志等信息以确定重点访问对象，制定针对性的访问计划，提高访问效率和准确性。

2.4. 技术水平及网络犯罪现场勘查水平的落后

由于网络犯罪的特性，网络犯罪现场勘查对勘查人员的技术性、专业性、规范性提出了更高的要求。这就使得网络犯罪现场勘查人员需要具备计算机相关的专业知识和技能。在网络犯罪现场勘查中，勘查人员需要对犯罪现场进行充分的分析判断，对犯罪现场进行全面、立体的勘查，获取一切与犯罪现场有关的电子介质、证据材料等，为现场分析提供依据。而在实际的勘查过程中，电子证据具有无形性、易篡改性、易破坏性的特点且极易被人为损坏，勘查人员的技术如何保证对网络犯罪现场物理空间以及虚拟空间进行细致全面的勘查以及如何保证电子介质中的原始数据不在勘查过程中被破坏是网络犯罪现场勘查的一大难点。当前，勘查人员队伍中传统的勘查技术不能满足高技术要求的网络犯罪现场勘查的需要，网络犯罪现场勘查经验不足，亟待提升勘查人员队伍技术水平。在当前云计算和大数据环境下，传统的电子数据取证技术需要大量时间对数据进行收集、处理与分析，难以高效应对海量数据的快速提取和分析，需要引入具有高效数据采集、数据分析、数据存储与结果输出能力的电子数据取证模型并能被勘查人员所掌握，以应对现有勘查技术与网络犯罪技术发展之间的矛盾。

2.5. 现场分析难度大

现场分析需要将网络犯罪现场勘查过程中从物理空间及虚拟空间中获取的线索及证据进行梳理及分析，构建网络犯罪的完整证据链条 [4]，从而确定犯罪行为的性质等，为侦查工作提供方向。在网络犯罪现场分析中，证据种类复杂多样且极易损毁，现场分析难度较大。勘查人员需要根据在虚拟现场中会获取到网站线索、即时通信软件、电子邮件线索、网上银行账户、网络日志等信息，将虚拟空间获取的证据与物理空间所获取的证据相匹配，判断是否为犯罪嫌疑人所留。例如，在跨境网络赌博案件中，勘查人员往往需要将服务器日志中的 IP 地址、交易记录与犯罪嫌疑人的物理活动轨迹、银行账户信息等进行关联分析，进行数据碰撞，不断完善完整的证据链条，这一系列分析过程需要勘查人员具有极高信息化侦查能力与现场分析能力。

2.6. 证据收集与固定困难

电子数据如今作为网络犯罪中的关键证据种类，对勘查人员的取证技术能力具有极高的要求。在电子数据取证内容上，勘查人员面临着电子数据如何提取与固定、如何保证电子数据原始状态不被破坏以及如何保证电子数据完整性等一系列难题。而在实践中，勘查人员队伍普遍不具备高水平的计算机技术能力，特别是在电子数据远程取证技术上的普及相对落后。滞后的技术水平无法适应计算机技术以及网络犯罪的高速发展，难以满足云取证工作的需要。在电子数据取证程序上，勘查人员还面临着电子数据取证程序不规范的问题。实践中勘查人员取证技术操作有误、网络在线提取替代网络远程勘验、忽视取证审批程序、滥用远程电子数据取证程序等问题，对证据效力以及公民信息数据权益均有着不当影响，勘查人员取证行为及取证程序亟待规范。

3. 网络犯罪现场勘查难点的解决对策

3.1. 提高网络犯罪现场的确定能力

对于网络犯罪现场的确定，从空间上可以将网络犯罪现场分为本地现场和远程现场。本地现场即为发现犯罪行为的计算机系统及其所在的物理空间。对于本地现场的确定应以该计算机为中心现场，向其他计算机进行辐射，判断案件中嫌疑人所用的计算机，从而确定本地现场。对于远程现场的确定，勘查人员可以通过技术手段确定嫌疑人作案所用的服务器IP地址从而确定嫌疑所用VPN的IP地，通过入侵VPN服务器日志嫌疑人的路由日志，从而确定远程犯罪现场的IP地址及ISP，最终锁定嫌疑人所处的实际位置即本地现场，基于此确定远程犯罪现场，并与本地现场进行比对。在美国司法部发布的过往案例中可以发现，其网络犯罪现场勘查中已采用“区块链+IPFS”混合存储技术，将VPN日志分布式存储于星际文件系统（IPFS）中，通过区块链存证能够有效确保日志完整性。该手段对于将IP地址与VPN日志相匹配、确定网路犯罪的远程现场有着重要

积极作用。区块链存证通过利用分布式存储等技术，将电子数据存储在区块链的链状结构之上，而每一个区块中会包含上一区块的哈希值和当前区块的数据信息，改动任何一个区块的信息则必须改后后续每一个区块的相关信息，因此，哈希值保证了存储的区块链数据不易被篡改 [5]，有效保障了区块链上电子数据的真实性。

3.2. 增强现场保护意识及规范水平

勘查人员在接到网络犯罪的报案或发现案件时，应当及时赶赴现场，在赶赴现场之后应对现场进行封锁，设立警戒线，杜绝无关人员进入现场，明确任何人未经许可不得进入案发现场，同时布置警力进行警戒，维持现场秩序，防止一切可能破坏网络犯罪现场的情况发生 [6]。

做好网络犯罪现场的基本现场保护之后，现场保护人员要确保中心现场内的人员不得随意接触计算机设备及现场电源开关，防止系统状态被改变、系统内文件和数据被增加、删除或修改，防止机内信息和机上的痕迹、物证遭到破坏，使相关计算机设备保持一个相对独立、隔离的原始状态。同时维持现场最初的开关机状态、网络连接状态、系统运行状态，使内存保留当前系统正在执行的任务、进程、临时文件等信息，排除系统断电等情况，确保系统保持静态，保证系统内易失数据不会损坏。随后，勘查人员才可按照操作规范进行电子数据的勘验检查及取证工作，保证电子数据的原始状态及其完整性。

如果系统受到的安全威胁、损害有进一步扩大或可能导致证据灭失的严重后果，应视情况断开网络，保护网络及其相关设备。

3.3. 组织开展科学有效的现场访问

组织开展科学有效的现场访问是获取关键证据、了解案情细节的重要途径。对于开展现场访问，首先要注意隔离在场人员。其次，明确访问目的并根据案件性质、现场情况制定有针对性的现场访问计划。接着，划定合适的访问范围。访问对象主要包括被害人、被害单位、网络管理人员、知情人等。但勘查人员可以根据案件具体情况筛选关键访问对象，筛选出与案件关系密切、可能掌握关键信息的知情人作为重点访问对象进行访问 [7]。访问过程中，勘查人员需要采取多种提问方式相结合的方式对访问对象进行引导与追询，充分重视被害人及知情人的心理状态，缓解被害人、知情人的紧张情绪，消除其顾虑，确保现场访问能够获取到相关线索。

3.4. 加强技术水平与勘验检查水平培训

第一，公安队伍需要进行技术创新与装备升级。各地勘查人员应聚焦现场勘查工作中存在的效率低、检验慢、智能化水平不高等问题，侧重网络犯罪案件现场取证方向的新技术和新装备的开发与应用。利用现代前沿科技成果，如大数据、人工智能等技术，构建“专业+机制+大数据”新型警务运行模式，大力推动智能化建设，加强协同作战能力，提高公安队伍新质战斗力，全面提升刑事案件的现场勘查质量。同时，推进电子物证、视频侦查等新技术专业实验室的建设，推动传统技术专业的现代化升级。例如，北京市公安局通过建立电子数据取证实验室，引入了人工智能证据分析系统，大大提高了网络犯罪案件的勘查效率和准确性。

第二，开展勘验检查技术培训及勘验检查技能大赛。通过专业课程和培训，提升刑事技术人员的网络犯罪案件现场勘查技术，提升一线勘查人员的技术能力。此外，开展勘验检查技能大赛可以提升勘查人员的现场勘查和提取检验能力。例如，山西公安通过组织全省预赛、决赛和集训备赛，提高了民警电信诈骗案件窝点现场勘查和电子数据检验鉴定能力水平。同时邀请国内外网络安全领域的专家学者进行授课和交流，交流分享最新的技术和实务案例，拓宽勘查人员的视野和思路。

3.5. 提高现场综合分析能力

网络犯罪现场分析的一大要点是通过网络信息分析嫌疑人特征。由于互联网的匿名属性，嫌疑人在网络上的言行一定程度上能真实地反应其性格特点、社会关系、心智能力等特征，甚至能记录嫌疑人的作案计划。侦查人员应当对网络犯罪现场获取的网络信息进行全面的分析，如嫌疑人的QQ、微信、微博等一系列社交软件聊天记录，微信、QQ、微博主页内容等，综合分析嫌疑人的特征。同时，还可以从获取的大量网络信息中，寻找发现、分析总结出嫌疑人的网络行为特征、网络技术掌握水平、是否记录有犯罪动向等信息，对嫌疑人进行画像，为后续侦查活动提供有力支撑。具体而言，通过信息化侦查手段对嫌疑人的网络数据进行采集、存储、分析和处理，从而分析嫌疑人的互联网用户行为模式、行为偏好和网络需求，以此对嫌疑人进行画像服务于网络犯罪现场分析。除此之外，现场分析的另一大要点是需要将本地现场的线索与远程现场的线索进行相互比对分析。分析判断本地现场所获取的物证线索能否与虚拟现场的电子数据相匹配，判断是何者犯罪嫌疑人所留以及其证明力度等信息。例如，通过比对本地图像提取的犯罪嫌疑人指纹与远程现场服务

器日志中记录的操作 IP 地址对应的上网设备 MAC 地址,成功锁定了犯罪嫌疑人使用的作案设备,增强证据的关联性和证明力,对两类网络犯罪现场所获取的线索进行综合分析。

3.6. 规范勘查人员取证行为

在电子数据证据的收集取证过程中,勘查人员应当保证电子证据的完整性、真实性、可再现性,对于网络犯罪现场中出现的一切电子数据要确保全面收集,以确保能够形成完整、有效的证据链条进入诉讼阶段。程序上,勘查人员取证时应当严格遵守《公安机关办理刑事案件电子数据取证规则》依法取证,保证证据合法有效。取证过程中如遇到专业技术问题有必要邀请技术专家参与时可以邀请,必要时邀请的专家可以作为专家证人进入司法程序。在实践中,可邀请网络安全领域的专家参与取证过程,对电子数据的技术特征和形成过程进行专业分析,确保证据的科学性和可靠性。证据内容要求上,电子数据证据强调数据原始性与证据的完整性,电子数据证据在取证全过程及后续一切司法程序中应当始终保证其内容不得发生过任何变化,在取证过程、现场分析、司法鉴定、移送审查起诉、证据展示等过程中均不得对数据造成任何变更。具体而言,可以采用区块链存证技术与哈希值校验技术相结合。正如前文所述,区块链上每一个区块中会包含上一区块的哈希值和当前区块的数据信息,改动任何一个区块的信息则必须改后后续每一个区块的相关信息[8]。因此,通过对提取的电子数据进行哈希值计算[9],并记录在取证报告中,能够有效确保数据在传输和存储过程中未被篡改,保证电子数据的原始性与可追溯性。最后需要注意的是,取证时应确保案件信息保密以及维护当事人的隐私权等合法权利。

4. 结语

随着网络信息技术的发展,网络犯罪手段呈现高技术性、隐蔽性、多变性的趋势。犯罪行为难以洞察,犯罪现场难以确定,对现场勘查工作提出了更高的要求。当前勘查队伍中技术水平及取证行为规范难以适应网络犯罪的发展演变,对于网络犯罪现场勘查中出现的难题亟待解决。希望本文对于解决对策的研究能对日后的网络犯罪现场勘查实践中的现场勘验检查及分析提供一定的帮助,规范勘查人员取证行为,提高勘查队伍网络犯罪现场勘查素质水平。未来,还需要持续关注网络犯罪的新趋势和新技术,持续优化和创新网络犯罪现场勘查的方法和手段,以更好地应对日益复杂的网络犯罪挑战。

参考文献

- [1] 许志.现场勘查[M].北京:中国政法大学出版社,2023:3.
- [2] 蒋占卿.计算机网络犯罪案件“虚拟空间”现场勘查研究[J].中国人民公安大学学报,2003(6):110-121.
- [3] 王明霞.网络犯罪现场勘查的重难点问题研究[J].广东公安科技,2020,28(3):65-67.
- [4] 吴燕波,向大为.论网络犯罪基本特征及侦查取证的一般要求和方法[J].法制与社会,2019(23):221-222.DOI:10.19387/j.cnki.1009-0592.2019.08.225.
- [5] 马骏,瑚峰.区块链存证之于刑事电子数据存证困境的突破[J].山西省政法管理干部学院学报,2023,36(2):58-62.
- [6] 吴伟宏,杨桂宾.浅论网络犯罪的特点及其现场勘查[J].法制与社会,2010(3):136.DOI:10.19387/j.cnki.1009-0592.2010.03.079.
- [7] 张天宇,单秉治.网络刷单诈骗犯罪现场勘查的困境与对策[J].北京警察学院学报,2023(6):102-107.DOI:10.16478/j.cnki.jbjpc.20231117.001.
- [8] 宋晶.大数据背景下刑事电子数据取证规范化研究[D].太原科技大学,2024.DOI:10.27721/d.cnki.gyzjc.2024.000376.
- [9] 孟启元.后疫情时代电信网络诈骗犯罪现场勘查的困境及对策研究[J].国际公关,2021(9):140-143.DOI:10.16645/j.cnki.cn11-5281/c.2021.09.047.