

# 暗网犯罪的成因及解决对策

王皓赞

上海政法学院刑事司法学院, 上海

收稿日期: 2023年7月7日; 录用日期: 2023年8月3日; 发布日期: 2023年8月15日

## 摘要

随着互联网的不断发展, 表网仅是出现在公众视野的冰山一角, 在水面下存在的深网与暗网才是互联网的大部分主体。暗网犹如潘多拉魔盒, 成为了互联网下的幽灵, 在暗网中黑灰产业横行, 恐怖主义、毒品犯罪、侵犯公民个人信息等各类犯罪充斥着暗网的各个角落。本文利用犯罪学中日常活动理论对暗网犯罪产生的原因进行分析。通过多元化治理的模式, 构建“产-官-学”三方多元合作机制, 注重对于青年人三观的培养, 增强我国电子数据相关技术的研究, 增强各国之间对于暗网犯罪打击的协作, 构建国际刑事司法协助, 构建起对暗网犯罪打击与治理相结合的协同新局面。

## 关键词

互联网, 暗网犯罪, 犯罪态势, 多元治理

# The Causes and Solutions of Dark Net Crimes

Haoyun Wang

College of Criminal Justice, Shanghai University of Political and Law, Shanghai

Received: Jul. 7<sup>th</sup>, 2023; accepted: Aug. 3<sup>rd</sup>, 2023; published: Aug. 15<sup>th</sup>, 2023

## Abstract

With the continuous development of the Internet, the table network is only the tip of the iceberg that appears in the public view, and it is the deep network and dark network that exist under the surface of the water that is the majority of the main body of the Internet. The dark net is like Pandora's Box, and has become a ghost under the Internet. In the dark net, the black and grey industry is rampant, and various crimes such as terrorism, drug crimes and infringement of citizens' personal information fill all corners of the dark net. This paper uses the theory of daily activities in criminology to analyse the causes of dark net crimes. Through a diversified mode of governance, a tripartite multi-faceted cooperation mechanism of "industry-government-academia" is built, with emphasis on the cultivation of the three views of young people, the research of electronic da-

ta-related technologies in China is enhanced, the collaboration between countries in the fight against dark net crimes is strengthened, and international judicial assistance in criminal matters is built, so as to build a new collaborative situation that combines the crackdown on dark network crimes with governance.

## Keywords

Internet, Dark Net Crime, Crime Situation, Multiple Governance

Copyright © 2023 by author(s) and Hans Publishers Inc.

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

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



Open Access

## 1. 引言

在互联网大数据时代，网络成为人们日常生活必不可少的工具之一，但随着互联网的发展，网络犯罪也逐渐发生，成为新型犯罪之一。网络具有匿名性、虚拟性等特点，使网络犯罪的案件侦破具有一定的难度。除明网外，世界上还存有暗网，随着 2015 年“章莹颖失踪案”轰动了全球后，该案涉及的“绑架 101”网站进入了我国大众的视野，此外随着国际其他国家对于网络犯罪的打击，如“阿尔法湾”、“丝绸之路”、“茶马古道”等暗网，暗网逐渐被我国大众所熟知，同时也促进了犯罪人使用暗网进行犯罪的行为的发生。暗网犯罪就犹如“潘多拉的魔盒”，因此，笔者将对暗网犯罪的成因进行分析，并以此提出治理建议。

## 2. 暗网的基本概述

### 2.1. 暗网的概念

“暗网”的概念在 20 世纪 90 年代被提出，但直到 2013 年美国著名暗网“丝绸之路”(Silk Road)的创始人乌布利希被捕，暗网才引起公众的普遍关注，而此时“丝绸之路”的匿名交易已达到 150 万笔，交易额超过 12 亿美元[1]。在现实生活中，我们可以根据互联网的访问权限，将互联网分为三类：表网、深网与暗网。

表网(the public web)指的是第一层次的网络，是我们平时连上 Wi-Fi 或是用流量便能够接触到的普通网络。表网是最被人们所熟知的普通网络，如谷歌、百度等。学术上，表网是指“已经被编入索引，利用百度、谷歌、雅虎等互联网标准搜索引擎和网络浏览器能够直接访问的页面和内容，主要以通过超链接方式关联起来的网页构成”[2]。

深网(deep web)是第二层网络。“深网”是不能使用标准搜索引擎索引的非表层网络[3]。有研究根据全球图书馆数据生成、拷贝和使用的储量进行估算，认为深网的规模约为可见网络的 400 倍[4]。例如，国家机关的内部网站、学校和科研机构的数据库等一些内部网站就是深网的组成部分。深网需要账号密码才能够访问，并且深网的建立依托于一定的数据技术。但在实践中，网络犯罪也会触及到深网的领域。

暗网(dark web)是第三层网络，许多学者以及研究者认为暗网是深网的一部分，但其具有更高的技术壁垒。暗网需要借助一定的辅助软件才能够登入，在现实中常用的是 TOR (洋葱路由浏览器)、I2P (隐形网)等辅助工具，只有使用特定的工具才能够有效访问网站。因此我们可将暗网视为有效的隐藏空间，这些特定工具会对节点进行分层，能够使用户信息难以泄露。

## 2.2. 暗网的特征

### 2.2.1. 隐匿性

暗网的核心特点便是具有隐匿性。不借助特殊的工具用户无法通过普通的技术手段进入暗网。暗网的辅助工具会给用户的数据、信息、联网地址进行加密，像洋葱一样分层加密，最终组成若干层，将用户的信息保护于中心。因此，经过多节点、多分布的层层加密，用户的 IP 地址、真实身份等重要信息就变得难以查明[5]。

### 2.2.2. 便捷性

暗网接入方式简单，通常不需要特别专业的计算机技能，技术门槛较低。多数人虽然不懂如何接入，但是通过 VPN 翻墙进入国外的许多论坛网站，如 Facebook、Twitter 等平台，在外网平台上存在许多链接暗网的教程，故用户不需要花费高额的培训费用，只需要翻墙在外网平台上下载普通软件，并按照教程步骤，就能够登入暗网。

### 2.2.3. 难以监管

暗网由于使用上述的特殊辅助工具，具有一定的技术壁垒，并且数据流存在保存时效，故对于监管部门而言，监管暗网具有一定的困难。

### 2.2.4. 跨国性

暗网的网络终端常设立于国外，并且暗网具有跨国性的特点，世界各地的人只需要具备辅助软件便能够在各地登入暗网，这也给监管带来了一定的难度。

### 2.2.5. 交易方式的特殊性

在暗网中，不像普通用户在使用普通网络使用支付宝、微信或是 visa 等方式进行付款。暗网中的交易使用了区块链技术。由于区块链采取点对点系统构架，组成的各个节点共享计算资源而不受中央节点的控制和协调，具有较好的抗操纵性和安全性，它不会拒绝某些用户使用其服务，对任何人开放，没有人能够阻止、关闭交易过程[6]。

## 3. 暗网犯罪的基本概述

### 3.1. 暗网犯罪的定义

目前我国学界以及国际上对于暗网犯罪并没有一个权威、统一的定义。通常认为，网络犯罪是指以网络为工具或对象，实施危害网络信息系统安全的犯罪行为[7]。有学者认为，暗网犯罪是指在网络空间中，利用暗网实施犯罪行为的犯罪[8]。也有学者认为，暗网犯罪是使用暗网空间的媒介手段进行的犯罪[9]。笔者认为，这两点均未能全面定义我国现今的暗网犯罪，对于暗网犯罪应作广义解释。笔者认为，暗网犯罪指的是利用特殊的工具登录暗网，利用暗网的特殊性质，将暗网作为犯罪工具在暗网上实施犯罪，或是将暗网作为犯罪对象的危害行为。暗网犯罪作为互联网犯罪的分支，有效地接入暗网，是犯罪人实施具体犯罪行为的起始点[10]。

### 3.2. 暗网犯罪的特征

#### 3.2.1. 暗网犯罪具有匿名性

暗网始于 ARPANET，它是互联网的始祖，这些具有隐匿性的网络成为美国海军的首选媒介，TOR 被称为“隐藏下载该软件的用户的位置和 IP 地址”，以保护海外的美国特工和持不同意见的政见者[11]。因此，暗网具有高度的私密性，使人难以追踪，暗网犯罪的犯罪人因此也具有匿名性的特征，使用特殊

的技术手段的暗网，能够使犯罪人的真实身份难以被追踪。

### 3.2.2. 暗网犯罪类型多样化

当然，除了强奸罪等必须以行为人自身或他人的人身作为犯罪工具的传统犯罪外，其他犯罪基本可以通过互联网实施[12]。在网络信息时代，普通表层网络上的犯罪类型也多种多样。暗网更是包含了表层网络所不能涉及的犯罪类型，毒品交易、淫秽色情信息、恐怖主义、分裂言论、公民个人信息、买凶杀人等充斥了暗网的各个角落。

### 3.2.3. 暗网犯罪交易方式的便捷性与隐蔽性

暗网犯罪的交易方式与普通犯罪的交易方式不同，普通财产类犯罪通常是通过抢劫、盗窃实物或是通过网络非法占有他人财物，使用的手段、媒介被普通人所熟知，如支付宝、信用卡等。而暗网犯罪多用虚拟货币进行交易，如比特币。与传统政府发行货币不同，比特币并不依赖于任何政府机构来发行，仅仅依赖于计算机算法[13]。比特币的特殊性能够去中心化，让交易难以寻觅。当暗网中双方达成买卖合意并且通过比特币进行交易，会随机生成比特币的可用地址。尽管区块链技术显示交易的记录，但是交易主体的身份信息仍然不能追踪。因此，暗网犯罪交易具有便捷性以及隐匿性的特征。

### 3.2.4. 暗网犯罪的跨国性特征

截至目前，我国破获的暗网犯罪，其网店终端多设立于境外，此外，暗网犯罪的犯罪人遍布全球各地，因此暗网犯罪具有明显的跨国性特征，这也给我国侦破暗网犯罪带来了一定的难度。

## 3.3. 暗网犯罪的主要犯罪类型

### 3.3.1. 毒品类犯罪

暗网毒品犯罪主要是通过暗网非法交易、走私毒品。犯罪人通过暗网与境外销售毒品的犯罪人取得联系，双方合意达成买卖并通过比特币等虚拟货币进行付款，随后，境外贩毒主体会通过各种渠道、形式将毒品寄至中国。例如暗网“丝绸之路”，丝绸之路市场拥有全球近 15 万名买家和近 4000 名供应商，他们在丝绸之路上讨论毒品效果、进行交易。

暗网犯罪不仅指发生在暗网上的犯罪，在暗网上直接经营犯罪业务，或从暗网获取犯罪方法，或利用暗网掩护其犯罪或资金转移，都属于暗网犯罪的范畴[14]。

### 3.3.2. 侵犯公民个人信息类犯罪

侵犯公民个人信息罪是我国暗网犯罪主要涉及的犯罪。在暗网中非法收售公民个人信息也是我国目前重点打击对象，如今年的净网行动以及侦破“茶马古道”等。犯罪人主要通过暗网获取能够突破企业公司的防火墙的木马软件，非法获取公民的个人信息，或是在暗网上购买公民个人信息，再通过暗网，将其转售给他人，进行盈利行为。

### 3.3.3. 恐怖主义犯罪

暗网中存有大量恐怖主义相关的视频、言论，以及教授恐怖主义犯罪的行为。该类犯罪主要是犯罪人在暗网中散布、宣传或是传播与恐怖主义有关的视频、言论以及资料。

### 3.3.4. 网络色情犯罪

网络色情犯罪是依托于互联网的新型犯罪形式。由于暗网的隐蔽性和跨国性特征，犯罪分子通常在境外构建其服务终端并定时更换域名，在暗网中此类犯罪更为广泛和隐蔽。暗网中的网络色情犯罪，包括但不限于网络色情直播、热舞、软色情、色情写真和自制淫秽视频等方式，满足观看者的猎奇心理，并以此牟取利益。

### 3.3.5. 财产型犯罪

暗网的出现给犯罪者带来了极大的便利，网络赌博、网络诈骗等也以此为依托而产生。利用暗网架构出网络赌博、诈骗等平台，不仅对公民的个人财产造成了侵害，也会造成国内财产的流失，同时也侵害了我国网络安全的法益。利用暗网进行网络博彩等犯罪，并多数使用比特币等虚拟货币进行交易，使得以暗网为依托的财产型犯罪更具有复杂性。

### 3.4. 暗网犯罪的危害性

暗网犯罪具有严重的社会危害性。

首先，暗网犯罪侵害了国家的公共安全。暗网由于其浏览器、辅助工具等的特殊性，使得暗网用户难以被追踪，许多国际恐怖组织、极端组织会通过暗网交流、买卖军火、甚至是获取各个国家的机密文件。由于 TOR 等技术的难以追踪性，导致了恐怖主义犯罪分子能够肆无忌惮地在暗网上寻找其需要的武器装备[15]。许多恐怖组织、极端组织，如伊斯兰恐怖分子，在暗网上招兵买马、宣传其组织的思想。

其次，暗网犯罪严重侵害了公民的人身安全。暗网市场上公民的个人信息、私密照片、虚假证件等都被明码标价。在暗网上买卖色情视频、个人信息或是买凶杀人、贩卖毒品是暗网的常态。这些违法犯罪行为均对公民的人身安全造成了重大的威胁。

最后，暗网犯罪侵害了公民的财产安全。在暗网中，形成了电信诈骗、信用卡盗窃等财产型犯罪的灰黑产业链。由于暗网技术的壁垒，使得这类侵害财产类案件难以被侦破，被害人的财产也难以被追回。

## 4. 暗网犯罪的产生原因

由上文可见，暗网犯罪在我国呈现的主要犯罪可分为以下几类：一是网络毒品犯罪，二是侵犯公民个人信息类犯罪，三是网络恐怖主义犯罪；四是网络色情类犯罪，五是财产型犯罪。根据理性选择理论，通过暗网实施以上几类犯罪，首先是犯罪成本低廉，犯罪人只需要通过 VPN 翻墙获取洋葱浏览器等暗网登入的必要软件，下载软件便可登入暗网；其次，犯罪人通过暗网犯罪可获取巨大的利益，如贩卖公民个人信息的利益极大；再次，暗网犯罪的风险也较小，暗网犯罪极为隐蔽、难以追踪的特性，致使暗网犯罪难以被侦破。

据此，笔者将运用日常活动理论分析暗网犯罪的产生原因。犯罪的日常活动理论是理性选择理论的另一发展，其基本观点认为，犯罪行为的发生与日常生活中的某些因素密切相关[16]。日常活动理论认为，犯罪发生必然存在三大要素，即有犯罪动机的人、合适的目标、以及缺乏有能力的监管者[17]。当该三要素同时具备时，则犯罪便会发生。

### 4.1. 犯罪人的原因

根据笔者的研究分析可知，暗网犯罪的犯罪人多为无业、文化程度较高的生活于互联网产业发达地区的年轻人。对于这类犯罪群体，因现在社会竞争激烈，对于学历的要求也越来越高，高中、大专或是大学毕业的人难以找到工作，犯罪人处于无业、务工的状态。由于收入来源不稳定，或甚至是毫无收入来源，又由于犯罪人接触了互联网上大量的不良信息或是受到了焦躁、金钱至上等理念的刺激，促使犯罪人产生了犯罪的动机。如今，微博、抖音等网络平台是年轻人热衷于分享生活、获取信息的渠道，但其中充斥着大量不正确的价值观，如炫富、不劳而获等内容，这些内容冲击着刚步入社会的年轻人的价值观，使他们逐渐产生赚块钱以实现财富自由的想法。暗网便是一个途径、渠道。在暗网中鱼龙混杂，在暗网这样的虚拟世界中容易产生兴趣、目标相同的亚文化群体。大部分犯罪人大量的时间未与社会发生正面接触，而互联网作为当下最容易接触到的虚拟世界，容易为犯罪人带来快感[18]。在暗网中，目标、

价值观相同的人群互相称赞或是传授犯罪手段，容易使犯罪人在心理上获取满足感。此外，暗网犯罪的犯罪人通常社会联系较弱，因其无业、务工等特征，往往无法与社会建立正常的联系，犯罪人因此逐渐远离正常的社会生活，在闲暇时间中长时间沉迷于网络。缺乏较强的社会纽带，就缺乏了正常的社会控制因素，因此也加大了犯罪的机率。

## 4.2. 合适的目标

根据日常活动理论的观点，犯罪人选择犯罪要有合适的目标，笔者认为，在暗网犯罪中，合适的目标因具备价值、可移动性、可接见性的特点，因此笔者将从该三点特征进行分析。

首先，暗网犯罪的目标具有价值性。在笔者上述文章中所整理的数据来看，暗网犯罪常涉及的犯罪类型，犯罪利益较高，可以使犯罪人获得精神、肉体以及物质的利益，即暗网犯罪的目标具有精神、肉体以及物质的价值。例如，暗网犯罪中的出售公民个人信息类犯罪，如2020年广西最高人民法院判处的一起案件中，犯罪人出售一万人的公民个人信息便能获得2150元的利益；2020年广州某法院判决的一起案件中，犯罪人一天内出售公民个人信息便能获得1万元的利益；同时，暗网中还存有大量淫秽色情信息、与我国社会主义相悖的恐怖主义、分裂国家的言论；暗网中还存在贩卖毒品等违禁行为。因此，犯罪人不仅能够通过暗网获得精神、肉体上的满足，也能通过暗网获取物质上的收益。

其次，暗网犯罪的目标具有可移动性。笔者认为，暗网犯罪通过网络虚拟货币进行交易，如比特币等，随后，犯罪人能将比特币与人民币进行转换。此外，在暗网中充斥着各类信息，犯罪人获取信息较为便捷、成本也较为低廉。因此，犯罪人无需耗费大量的精力，便能因暗网的便捷性以及货币变现的快捷性获取利益，在一定程度上也刺激了犯罪人的犯意。

最后，暗网犯罪的目标具有可接见性。暗网犯罪只需要VPN和浏览器便能够进行，同时因暗网的特殊性、隐匿性、私密性很难被侦查，在互联网上难以定位，因此犯罪人的风险较小，犯罪人能够隐匿的可能性较大。

## 4.3. 缺乏监管

暗网缺乏我国有关部门的理由监管，同时暗网犯罪的取证存在困境。网络犯罪的取证要求时效性，若是在有效时间内没有完成取证工作，那么数据节点存在被覆盖的可能。暗网犯罪具有安全性、身份验证、匿名性、虚拟货币和隐藏交换等五个方面的独特属性，又决定了暗网在取证载体、证据元素、证据存储形式等方面与互联网犯罪电子取证存在较大差异[19]。同时暗网的数据存储介质极不稳定，若是暗网终端后台发现有人从外部非法入侵试图调取证据，那么相关数据将会被删除。这均给暗网的取证与监管带来了困境。

综上，笔者认为在犯罪人社会纽带较弱、工作收入不稳定的情况下，极易受到亚文化、网络平台中不良信息的影响，在网络犯罪的监管、取证存在困境，且暗网犯罪难以被侦破的情况下，犯罪人极易利益暗网实施犯罪以获取巨大的经济利益或是心理上的满足，暗网犯罪因此产生。

## 5. 暗网犯罪的多元治理模式

暗网犯罪是近年来的新型犯罪，并且随着互联网产业的不断发展，暗网技术以及信息隐匿技术也会不断发展，给打击治理暗网犯罪带来新的挑战。笔者认为，暗网犯罪的治理可以结合情境预防、多元治理理论进行构建。打击和防范暗网犯罪需要在政府主导、多方参与下，才能取得实效[20]。

### 5.1. 引领、培养青少年的价值观，免受亚文化的冲击

暗网中充满着亚文化的价值观念，暗网也是主要源于“网络朋克”，这一亚文化观点与主流文化相

差甚远,两者之间存在冲突。暗网包含着多种亚文化,如暴力亚文化、毒品、色情、猎奇事物、恐怖主义等等。这些亚文化思想对于暗网犯罪的发展起到了潜移默化的作用,逐渐形成犯罪思想及其行为模式,因而必须防止暗网亚文化思想的冲击[21]。暗网犯罪多发于青年群体,因此要积极引领、培养青年的价值观。笔者认为,需要倡导主流文化观点,目前艺术载体多样化,可以通过网络、书籍、杂志、电影、绘画艺术等多方进行主流价值观点的引导。学校、社会应加强对于大众的引导以及科普,普及暗网的危害性以及其负面影响。

## 5.2. 构建网络全媒体格局, 加强群体的社会纽带

笔者上文所述,暗网犯罪的产生原因之一是由于犯罪人的社会联系较弱,而暗网亚文化群体给予其归属感、满足感,获得认同感的犯罪人会逐渐越来越向暗网亚文化群靠近。因此,笔者认为在网络空间中,要加强正能量以及正确价值观的互动。让这些亚文化群体也能够参与到正常社会的网络互动中,可以通过组织线上活动等方式,促进亚文化群体与主流群体之间的良性互动,树造健康、向上的网络环境。帮助犯罪人融入社会,建立社会纽带,同时也能够帮助潜在犯罪人加强社会纽带的联系,去除该群体的负面情绪。

## 5.3. 建立专门部门, 对暗网犯罪进行监测

目前我国对于网络安全的治理主要依靠公安部网络安全保卫局、地方的网络安全总队、网络安全支队以及网络安全大队。四级管理体系构成了我国对网络犯罪监管的主力军,然而,虽然针对总体意义上的网络犯罪的执法机构已经确立,但具体到暗网犯罪时,我国尚未成立相应的机构,仍处于接收国外情报线索的被动应急阶段[22]。网安部门除暗网犯罪外,主要负责监测、侦查普通网络犯罪,普通的网络犯罪也层出不穷,暗网犯罪甚至存在更高的技术壁垒,侦查的难度更大。技术难题已成为网安工作人员侦查暗网犯罪的一道鸿沟。

笔者认为,对于暗网犯罪的侦查可以借鉴其他国家的做法,建立起更有效的打击路径。目前全球各国都对于暗网的打击力度愈发严厉,相应的措施也随着科技的发展在逐步升级。2017年美国协同欧洲刑警组织打击“阿尔法湾”,并成功将其侦破,隶属于欧洲刑警组织的机构——欧洲网络犯罪中心,便一致致力于打击暗网,其提倡建议建立起协调合作的途径,以增加执法的有效性,在2018年,该倡议落地实施,欧洲建立了一个调查小组,其具有专门的职能用以专门侦查暗网犯罪。同样,2017年的英国也成立了相关的部门——暗网情报部门,该部门隶属于英国国家犯罪局,该部门的职能主要是潜入暗网收入信息,在要打击暗网犯罪时便要起到积极的协同作用,协调其他部门进行活动。德国、日本也存在类似的机构对暗网犯罪进行打击。

因此,在暗网犯罪逐渐发展到全球时,我国也不能独善其身,应当积极投入到暗网犯罪的全球治理中。故笔者建议,各级网络安全部门之下应学习域外经验,设立专门的暗网调查小组或职能部门,专门潜入暗网收集有关暗网犯罪的情报信息、监测暗网中的网络犯罪活动,以此加强我国对于暗网犯罪的打击力度。

## 5.4. 建设“产-官-学三方互相协作学习机制”

暗网犯罪具有高科技的特征,有较高的技术堡垒,往往暗网犯罪的犯罪人所使用的犯罪手段具有高科技的特性,其使用的技术超出了侦查人员的能力范围,运用侦查人员的现有知识以及能力难以对暗网犯罪进行侦查。此时,我国网安局以及其他相关部门的工作人员不具有相应的技术能力。笔者认为,应当积极向具备计算机专业技能的专业人员寻求帮助。建立“产-官-学”相结合的模式,让专业的机构

及其人员提供技术支撑，能够帮助我国执法机关攻破技术堡垒。

例如，在欧美国家，美国便建立了这种模式。在美国，微软公司等计算机企业与部分高校，在美国联邦调查局的领导下，组成了网络执法培训联盟，有专业的机构、人员对警察进行专业技能的培训，同时专业机构及其人员在日常中也会致力于情报工作的收集。在亚洲的日本也具有相类似的模式。日本成立了日本网络犯罪中心，该中心的组成不仅包括专业的执法者，还包括高校、计算机互联网企业。并且在日本警察厅领导下，中心的计算机专业领域成员提供专业的技术，并研究新技术用以攻克网络犯罪的堡垒。英国也成立了由政府、企业以及高校组成的相应机构。

在我国尚未成立相应的机构，相应的运作机制尚未能够运用到打击暗网犯罪的实践中。我国目前仅成立了中国人民公安大学网络安全与犯罪研究中心，该中心除高校外，相关的科研企业也参与其中，但我国的国家机关并未参与其中。我国国家机关的执法者拥有专业的侦查能力，但是在暗网犯罪中，缺乏一定的专业技术，故需要专业的技术人员提供技术的支撑。打击暗网犯罪不能仅依靠执法者与法律，在互联网时代，还应当依靠科学技术。技术的落后限制了我国打击暗网犯罪的有效性，同时也限制了我国对于暗网犯罪的监管。

因此，笔者认为要积极构建“产-官-学”的合作模式，让科研机构、高校的专业人员参与到打击暗网犯罪中，充分发挥专业人员的优势，获得专业人员的技术支撑，加强对于暗网犯罪的打击力度。

### 5.5. 增强各主体之间信息的透明度，升级电子取证技术

相对于传统犯罪调查取证技术而言，网络犯罪对电子取证技术的要求，会随着互联网科技的不断发展而不断提高。但在网络犯罪，特别是暗网犯罪这一方面上，我国执法机关的取证技术难以突破犯罪手段的技术堡垒。虽然我国目前强调、重视对于电子证据的收集、取证，但是由于缺少专业人士的介入，我国电子取证技术发展较为缓慢。目前，我国公安部设立了专门的电子证据研究中心，其隶属于第三研究所，主要研究电子数据的收集、保存等方面；同时，我国地方各级公安也成立了多家实验室，用于研究电子数据方面的难题，如取证、鉴定、保存等。但对于电子数据、互联网方面的研究，我国的司法机关并不处于领先地位，在互联网技术方面，我国的相关科研机构处于领先地位，如厦门美亚柏科信息股份有限公司属于技术的龙头企业。同时，在实践中，我国执法机关也常会遇到取证难，相关主体不配合的情况。因此，在此基础上，应当公私合作，各主体之间加强其信息的互通，明确执法者的信息共享范围，确保执法者拥有畅通的信息共享途径，使网络犯罪中的取证、举证不再是一道难题。

### 5.6. 促进我国与国际间的刑事司法协作

由于暗网犯罪具有跨地域性、跨国性等的特点，难以将暗网犯罪的犯罪地点划于具体的某一国家之内。暗网犯罪通常涉及的国家、地区极为广泛。例如，笔者前文所述的毒品犯罪，牵涉极为广泛，通常毒品均由境外的毒枭提供，毒枭又遍布全球，但他们都通过暗网这一途径进行违法犯罪行为。通过在边境设卡等方式预防暗网上的毒品类犯罪不是最优选择。打击暗网犯罪，不仅要治标，也要治本。例如，欧洲成立的中心，对于暗网犯罪的打击力度以及有效性全球共睹，对于“阿尔法湾”等暗网的打击，离不开国际刑事司法的协作，仅仅依靠单一国家的力量，很难从根上将一个暗网连根拔起。

我国应紧跟全球警务时代的浪潮，与各国建立起国际刑事司法协作，对暗网犯罪进行打击。目前，联合国存在《联合国打击跨国有组织犯罪公约》作为跨国打击的指导，但是由于各个国家的国情、法律法规等各方面都存在着差异，在实践中，很难达成共识。但这并不意味着，要放弃国际刑事司法协作。笔者认为，各国应当在维护国家主权的前提下，对打击暗网犯罪这一方面进行协商，共同面对暗网犯罪所带来的挑战，如情报共享、技术合作等问题，弥补单独国家对暗网犯罪侦查、监测的不足，加强对于



暗网犯罪的打击力度，建立有效的、针对暗网犯罪的国际合作模式。

### 5.7. 增强对虚拟货币的管理

暗网犯罪的交易主要使用的是比特币等虚拟货币。虚拟货币在我国目前尚未存在有效的监管措施。我国目前《关于进一步防范和处置虚拟货币交易炒作风险通知》，其中警告了虚拟货币不被我国所认可，不能够在市场上流通。但是在暗网犯罪中，存在这其特殊的虚拟货币与人民币之间的转换模式，故应从源头上加强对于虚拟货币的金融监管。

### 5.8. 加强对网络灰黑产业的打击力度

在本文上述研究调查中发现，我国暗网犯罪的类型主要涉及侵犯公民个人信息。犯罪人在暗网平台上非法出售、购买公民个人信息以获取经济利益。公民个人信息的贩卖一直是我国网络灰黑产业链的顽疾。因此，要治理暗网犯罪，也要增大对于网络灰黑产业链的打击。类似于电信诈骗、公民个人信息的售卖在我国已形成一定规模的产业链，从源头打击此类犯罪，能够在一定程度上治理暗网犯罪的现状。

### 5.9. 我国境内建立多元的治理模式

普通群众应当倡导良好的网络氛围，同时对于网络上有关暗网以及暗网犯罪的信息要积极举报。警民合作的模式能够提高对暗网犯罪的打击力度。仅依靠我国执法机构对于暗网的监控以及侦查是不够的，还会存在大量的暗网犯罪黑数。因此，大众在平日使用互联网的过程中，遇见违法信息、有关的暗网犯罪的信息要及时、积极向执法机关举报。其次，作为国家的执法机关，应当加强对于暗网犯罪的打击，对于网络犯罪的普法教育，让群众了解犯罪的后果，扼杀犯意的产生。最后，在技术方面，各科研机构也应当加强对于暗网犯罪有关互联网技术的研究与开发。治理暗网犯罪需要依靠多方面的协调作战，才能从源头上对其进行根治。

### 5.10. 加重对于网络犯罪的处罚力度，增加有关暗网犯罪的法律条款

目前我国并没有针对暗网犯罪的法律条款的出台，但西方国家对于暗网犯罪均有严格的管控措施。虽然美国并未禁止其国民使用暗网，但是美国对于暗网上的内容会实施监听。我国目前仅对网络犯罪的个别犯罪行为进行了规制，但对于使用 VPN 翻过防火墙浏览外网、下载相关的登入暗网有关工具的行为，我国刑法并未将其规定为犯罪。虽然我国对于 VPN 持否定态度，但是具体落实到哪一刑法条款还有待商议。故笔者认为，应当适当增加有关暗网犯罪的刑法条款。增加犯罪人的犯罪成本，控制犯罪人进入暗网的途径，通过刑罚的一般作用与特殊作用对犯罪人进行威慑，挤压犯罪人的犯罪空间，起到打击暗网犯罪的作用。

## 6. 结语

大数据时代，互联网渗透到绝大多数人的日常生活中，成为人们生活不可或缺的一个部分。随着互联网技术的不断发展，暗网犯罪的科技壁垒也不断提高。暗网犯罪作为新型犯罪，我国对于暗网及其暗网犯罪的研究也处于不断探索的阶段。暗网犯罪具有匿名性、高科技性、多样化等特点，并且具有极大的社会危害性，不仅侵害了国家安全，还对我国公民的人身、财产安全的法益造成了损害。目前我国暗网犯罪的犯罪数量呈上升趋势，犯罪人多为收入不稳定的青年群体，出于对犯罪的成分、利益以及风险三方面的衡量，最终选择实施暗网犯罪。本文仅研究了暗网犯罪的一部分，还存在不足之处。在现有的研究基础之上，笔者提出了对于暗网犯罪的治理建议，通过运用情景预防、多元治理以及刑罚的作用，在暗网犯罪的监管、侦查以及国际刑事司法协作方面均提出了对策建议。只用通过加强社会边缘群体与

社会之间的纽带联系、构建“产-官-学”三方合作机制、提高我国对于电子数据的专业技术研究；同时，也要应当注重暗网犯罪的源头治理，如对现存的网络灰黑产业链的打击、对于网络虚拟货币市场的金融监管；最为重要的是构建起国际刑事司法协作。打击暗网犯罪需要国际各国之间的共同努力，中国不能独善其身，构建国际刑事司法协作，符合中国国家总体安全观的思想。从严、从本，打击与治理相结合，以期能够从源头上对暗网犯罪予以打击、治理，营造出良好、健康的网络环境。

## 参考文献

- [1] Bartlett, J. (2015) *The Dark Net: Inside the Digital Underworld*. William Heinemann Ltd., London.
- [2] Robertson, J. (2016) Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence. *The Cyber Defense Review*, **1**, 95-122.
- [3] 王枫梧. 我国暗网犯罪现状、治理困境及应对策略[J]. 中国人民公安大学学报(社会科学版), 2022, 38(1): 12-19.
- [4] 匿名者. 深网 Google 搜不到的世界[M]. 北京: 中国友谊出版公司, 2016.
- [5] 王子杰. 我国暗网犯罪的态势、特征及对策研究[J]. 河南警察学院学报, 2021, 30(5): 47-53.
- [6] 丹尼尔·德雷舍. 区块链基础知识 25 讲[M]. 马丹, 等, 译. 北京: 人民邮电出版社, 2018.
- [7] 张远煌. 犯罪学[M]. 第三版. 北京: 中国人民大学出版社, 2015.
- [8] 焦康武. 总体国家安全观视域下我国暗网犯罪应对研究[J]. 犯罪研究, 2017(6): 78-89.
- [9] 麦政. 暗网犯罪及其应对措施[J]. 中国刑事警察, 2020(1): 57-59.
- [10] 吴予轩. 暗网犯罪治理的国际法制研究[D]: [硕士学位论文]. 广州: 广东财经大学, 2019.
- [11] Lacson, W. and Jones, B. (2016) The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *International Journal of Cyber Criminology*, **10**, 40-61.
- [12] 喻海松. 网络犯罪十二讲[M]. 北京: 法律出版社, 2018.
- [13] 姚国章, 赵刚, 唐宝, 等. 比特币: 潮起潮落后的理性思考[J]. 南京邮电大学学报(人文社科版), 2014, 16(1): 46-55.
- [14] 焦康武. 总体国家安全观视域下我国暗网犯罪应对研究[J]. 犯罪研究, 2017(6): 78-89.
- [15] 程聪慧. 网络恐怖主义的挑战及其防范[J]. 情报杂志, 2015(3): 10-20.
- [16] 吴宗宪. 西方犯罪学史[M]. 第二版. 北京: 中国人民公安大学出版社, 2010.
- [17] 程薇, 吴建平. 国外犯罪时空分布研究综述[J]. 世界地理研究, 2013(2): 151-158.
- [18] 施展. 暗网犯罪研究[D]: [硕士学位论文]. 上海: 华东政法大学, 2021.
- [19] 郑荣哲, 滕兴华, 匡敬洪. 暗网犯罪案件取证警务实战应用研究[J]. 警察技术, 2022(1): 58-61.
- [20] Pattavina, A. (2005) *Information Technology and the Criminal Justice System*. Sage Publications Inc., Thousand Oaks. <https://doi.org/10.4135/9781452225708>
- [21] 钱敏. 暗网犯罪: 网络犯罪的深层探析[J]. 犯罪学论坛, 2018(5): 793-804.
- [22] 陈璐. 暗网犯罪与多元治理: 挑战与出路[J]. 铁道警察学院学报, 2019, 29(1): 83-90.