VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

Bakalářská práce

Možnosti odhalování obchodování s nelegálními látkami na darknetových tržištích

Autor práce: Dominik Drož, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Dominik Drož, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Možnosti odhalování obchodování s nelegálními látkami na darknetových tržištích

Název bakalářské práce v anglickém jazyce: Possibilities For Detecting The Trade In Illegal Substances On Darknet Marketplaces

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): Leden 2026

Cíl bakalářské práce:
Cílem bakalářské práce je zhodnotit současné možnosti odhalování obchodování s nelegálními látkami na darknetových tržištích se zaměřením na využívané metody, nástroje a postupy bezpečnostních složek České republiky a na základě zjištěných poznatků navrhnout opatření ke zvýšení efektivity odhalování této formy trestné činnosti.

Student: Dominik Drož	7.1.2026	Drož
Vedoucí práce: RNDr. Růžena Ferebauerová	7.1.2026	Ferebauerová

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	22.1.2026	
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	22.1.2026	
Rektor: doc. Ing. Jiří Dušek, Ph.D.	1.2.2026	

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. V platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. Zveřejněny jsou posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji doktorce Růženě Ferebauerové za cenné rady, připomínky a vedení této práce.

ABSTRAKT

DROŽ, D. Možnosti odhalování obchodování s nelegálními látkami na darknetových tržištích: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 62 s.

Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Bakalářská práce se věnuje problematice nelegálního obchodu s látkami na darknetových tržištích a možnostem jejich odhalení orgány činnými v trestním řízení. Teoretická část popisuje technické aspekty anonymizačních sítí, například sítě Tor, a roli kryptoměn při zakrývání finančních toků. Analyzuje také právní rámec České republiky, zvláště operativně-pátrací prostředky a mezinárodní spolupráci.

Praktická část, založená na případových studiích, zkoumá úspěšné mezinárodní operace proti darknetovým tržištím a faktory vedoucí k odhalení pachatelů. Na závěr jsou navržena opatření ke zvýšení efektivity boje s touto formou kyberkriminality v ČR.

Klíčová slova: návykové látky, blockchain, darknet, drogová kriminalita, kryptoměny, síť Tor.

ABSTRACT

DROŽ, D. Possibilities of Detecting the Trafficking of Illegal Substances on Darknet Marketplaces: bachelor's thesis. České Budějovice: College of European and Regional Studies, 2026. 62 pp.

Bachelor's thesis supervisor: RNDr. Růžena Ferebauerová

The bachelor's thesis addresses the issue of illegal trade with substances on darknet marketplaces and the possibilities for their detection by law enforcement authorities. The theoretical part describes technical aspects of anonymisation networks, such as the Tor network, and the role of cryptocurrencies in obscuring financial flows. It also analyses the legal framework of the Czech Republic, particularly operational and investigative methods and international cooperation.

The practical part, based on case studies, examines successful international operations targeting darknet marketplaces and the factors that led to the identification of offenders. Finally, measures are proposed to increase the effectiveness of combating this form of cybercrime in the Czech Republic.

Keywords: addictive substances, blockchain, darknet, drug crime, cryptocurrencies, Tor network.

Obsah

Úvod

Fenomén drogové kriminality prošel v posledním desetiletí zásadní transformací. Zatímco v minulosti byl obchod s nelegálními látkami spojen primárně s fyzickým kontaktem ohledně pouliční distribuce, současný trend ukazuje na masivní přesun do digitálního prostředí, konkrétně do šifrované sítě darknetu. Tato oblast, charakteristická vysokou mírou anonymity, představuje pro orgány činné v trestním řízení (OČTR) bezprecedentní výzvu. Tradiční metody operativně-pátrací činnosti narážejí na technologické bariéry, jako je vícevrstvé šifrování datového provozu nebo využití decentralizovaných kryptoměn, které efektivně maskují identitu aktérů i finanční toky.

Předkládaná bakalářská práce se zabývá problematikou odhalování této trestné činnosti z pohledu moderní kriminalistiky a bezpečnostních studií. Hlavním motivem pro volbu tohoto tématu je narůstající sofistikovanost pachatelů, kteří využívají platformy jako Tor či I2P k distribuci omamných a psychotropních látek v globálním měřítku. Práce se nepokouší pouze o teoretický popis fungování darknetových tržišť, ale klade si za cíl analyzovat konkrétní postupy, které umožňují prolomení této zdánlivé anonymity a zajištění důkazních prostředků pro potřeby trestního řízení.

Téma této práce je aktuální především s ohledem na rostoucí digitalizaci kriminality a její přesun do online prostředí.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Cílem této práce je detailně analyzovat současné metodické a technické možnosti identifikace a odhalování distribuce nelegálních látek na darknetových tržištích, zejména z pohledu mezinárodní policejní spolupráce. Výzkumné otázky jsou zaměřeny na identifikaci klíčových postupů, které vedou k prolomení anonymity pachatelů, a na posouzení efektivity existujících legislativních a operativních nástrojů v boji proti anonymizovaným digitálním trhům. Při zpracování práce jsem se zaměřil zejména na praktické aspekty vyšetřování této trestné činnosti.

Metodologicky je práce koncipována jako teoreticko-analytická studie. První část využívá literární rešerši a komparaci odborných zdrojů, včetně aktuálních reportů agentur Europol a UNODC, k vymezení teoretického rámce zkoumané problematiky.[1]

Praktická část aplikuje metodu případové studie zaměřenou na významné zásahy proti darknetovým tržištím v nedávné minulosti. Analýza těchto případů identifikuje klíčové faktory vedoucí k úspěšné identifikaci pachatelů, a to jak v oblasti technické analýzy blockchainu, tak při využití institutu předstíraného převodu a dalších operativně-pátracích prostředků.

[1] PÁNA, Lubomír a Miroslav SOMR. Metodologie a metody výzkumu. České Budějovice: VŠERS, 2007. s. 12–25. ISBN 978-80-86708-52-2.

2 Teoretická východiska kybernetické bezpečnosti a fungování darknetu

Tato kapitola se zaměřuje na základní principy, které umožňují fungování darknetu a s ním spojených aktivit. Pro pochopení způsobů, jakými bezpečnostní složky tyto činnosti odhalují, je nejprve nutné vysvětlit technologické i bezpečnostní souvislosti.

2.1 Kybernetická bezpečnost a její základní pilíře

Kybernetickou bezpečnost dnes nelze chápat pouze jako technickou oblast. Jde o širší soubor opatření, jejichž cílem je ochrana dat, systémů a uživatelů v digitálním prostředí.[2]

Základem je tzv. CIA triáda, která zahrnuje tři hlavní principy:

- **Důvěrnost (Confidentiality):** Přístup k informacím mají pouze oprávněné osoby
- **Integrita (Integrity):** Data nesmí být neoprávněně změněna
- **Dostupnost (Availability):** Systémy a data musí být dostupné v době potřeby[3]

V prostředí darknetu jsou tyto principy často využívány opačně – tedy k ochraně anonymity pachatelů a skrytí jejich činnosti.

2.1.1 Stratifikace webu a vymezení darknetu

Internet lze rozdělit do několika vrstev:

1. **Povrchový web (Surface Web):** Běžně dostupná část internetu, kterou indexují vyhledávače.
2. **Hluboký web (Deep Web):** Obsah, který není veřejně indexovaný (např. databáze, e-maily)

[2] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. 6., doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, 2025, s. 281.

[3] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019, s. 46-56.

3. **Darknet:** Záměrně skrytá část hlubokého webu, která k přístupu vyžaduje specifický software a protokoly.[4]

Darknet je tvořen skrytými službami a prostředími, která nejsou běžně dostupná standardní webovou navigací a často vyžadují zvláštní přístupové nástroje.[5]

2.1.2 Kryptoměny jako nástroj finanční anonymity

Kryptoměny hrají v prostředí darknetu zásadní roli. Umožňují provádět platby bez nutnosti zapojení bank nebo jiných institucí.

- **Blockchain:** veřejná a neměnná účetní kniha všech transakcí. Přestože jsou transakce dohledatelné, identity uživatelů jsou skryté za adresami.

- **Anonymizace plateb:** Pro zvýšení anonymity využívají pachatelé tzv. Privacy coins (např. Monero), které skrývají výši částky i adresy odesílatele a příjemce přímo na úrovni protokolu.[6]

2.2 Darknet a ekosystém nelegálního obchodu

Darknet není pouze technologické prostředí, ale tvoří i specifický ekosystém, ve kterém fungují různí aktéři – od prodejců až po administrátory tržišť.

2.2.1 Vymezení a stratifikace kybernetického prostoru

Kybernetický prostor je vhodné vnímat jako prostředí vznikající propojením digitálních dat, komunikačních toků, zařízení a infrastruktury, které spolu navzájem interagují bez ohledu na klasické geografické hranice.[7]

Z pohledu vyšetřování je důležité rozlišovat mezi digitální vrstvou (data, komunikace) a fyzickou infrastrukturou (servery, zařízení).

---

[4] ABU AL-HAIJA, Qasem et al. SafeSurf Darknet 2025: A Novel Dataset for Darknet Traffic Detection and Analysis. Preprints, 2025, s. 2.

[5] CHEN, Hsinchun. Dark Web: Exploring and Data Mining the Dark Side of the Web. New York: Springer, 2012, s. 46.

[6] CHAINALYSIS. *2025 Crypto Crime Mid-Year Update* [online]. New York: Chainalysis Inc., 2025 [cit. 2026-02-08]. Dostupné z WWW: https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/

[7] HRŮZA, Petr a kol. Kybernetická bezpečnost II. Brno, 2013, s. 9–11.

2.2.2 Evoluce a fungování darknetových tržišť (DNM)

Významným milníkem byl vznik tržiště Silk Road v roce 2011.[8]

To poprvé spojilo anonymitu sítě Tor s kryptoměnami.

Současná darknetová tržiště fungují podobně jako běžné e-shopy:

- Uživatelé mají účty
- Existují recenze prodejců
- Využívá se systém úschovy peněz (escrow)

Tento model zvyšuje důvěru mezi anonymními uživateli a umožňuje fungování trhu i bez přímého kontaktu.[9]

2.2.3 Kryptoměny jako nástroj zastírání finančních toků

Ačkoli bývá Bitcoin veřejností často spojován s anonymitou, přesnější je označení pseudonymní systém, protože transakce jsou veřejně zaznamenány a při dostatku doplňujících údajů je možné je zpětně spojovat s konkrétními osobami nebo aktivitami.[10]

S rostoucí možností analyzovat bitcoinové transakce se část uživatelů darknetu přesunula ke kryptoměnám, které kladou větší důraz na soukromí. Typickým příkladem je Monero, jehož konstrukce ztěžuje dohledání transakčních vztahů mezi odesílatelem, příjemcem a převáděnou částkou.

Pro OČTR (orgány činné v trestním řízení) to znamená, že klasická metoda „follow the money“ (sledování peněz) naráží na technologický limit, kdy nelze bezpečně prokázat propojení mezi peněženkou kupujícího a prodejce bez zajištění koncového zařízení. Tyto nástroje výrazně komplikují práci vyšetřovatelů.[11]

2.2.4 Právní rámec nelegálního obchodu v digitálním prostředí

V České republice je tato problematika řešena zejména trestním zákoníkem, konkrétně ustanovením § 283.[12]

---

[8] STROUKAL, Dominik. Dark Web: Sex, drogy a bitcoiny. Praha: Grada, 2020, s. 23-25.
[9] STROUKAL, Dominik. Dark Web: Sex, drogy a bitcoiny. Praha: Grada, 2020, s. 23-33
[10] ANYCOIN. Bitcoin není anonymní a zločinci to dobře vědí [online]. [cit. 2026-03-27]. Dostupné z: https://www.anycoin.cz/blog/blog-btc-anonymita?locale=cs_CZ
[11] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019, s. 130.
[12] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, § 283.

Specifikem darknetu je, že trestná činnost probíhá online, často přes hranice států. To komplikuje určení jurisdikce i samotné dokazování.

2.3 Modus operandi aktérů v digitálním a fyzickém prostoru

Analýza způsobu páchání trestné činnosti (modus operandi) v prostředí darknetu vyžaduje komplexní pohled, který kombinuje technické aspekty kybernetické bezpečnosti s tradičními kriminalistickými postupy. Pachatelé v tomto prostředí neřeší pouze samotnou distribuci OPL, ale primárně zajištění vlastní neodhalitelnosti skrze vrstvení bezpečnostních opatření.

2.3.1 Operační bezpečnost (OPSEC)

Zásadní roli hraje tzv. Operační bezpečnost (OPSEC).

Pachatelé:

- používají anonymní operační systémy (např. Tails)
- kombinují VPN a síť Tor
- minimalizují digitální stopy

Cílem těchto opatření je co nejvíce ztížit propojení online aktivit s reálnou identitou pachatele.

Z právního pohledu tato anonymita výrazně ztěžuje proces ztotožnění konkrétní fyzické osoby s aktivitou v kyberprostoru. Anonymita v kyberprostoru není absolutní, ale výrazně zvyšuje nároky na zajišťování důkazů, které musí být získány v souladu s trestním řádem, aby byly procesně použitelné. Používání více navazujících anonymizačních vrstev výrazně komplikuje proces ztotožnění konkrétní osoby s aktivitou v kyberprostoru. Vyšetřování se proto často neposouvá průlomem samotné technologie, ale až propojením technických stop s chybou pachatele nebo s důkazy z fyzického světa.

2.3.2 Psychologické faktory

Anonymita v online prostředí může posilovat tzv. online dezinhibici, tedy tendenci chovat se odvážněji a podstupovat vyšší míru rizika než v běžném osobním kontaktu. V prostředí darknetu navíc vznikají komunity, v nichž si uživatelé vyměňují zkušenosti, hodnotí prodejce a postupně budují určitou míru vzájemné důvěry.

2.3.3 Distribuce v České republice

Za nejzranitelnější část celého distribučního řetězce lze považovat okamžik, kdy se online komunikace a objednávka promění ve fyzické doručení nebo ukrytí zásilky. Právě v této fázi se anonymní digitální prostředí nejčastěji propojuje s reálným jednáním pachatele, tedy moment odeslání zásilky. V podmínkách České republiky se v odborné a bezpečnostní praxi objevují zejména tři distribuční modely:

1. **Klasické poštovní služby:** V některých případech bývají zásilky upravovány tak, aby bylo jejich odhalení při přepravě obtížnější. Nelegální látky mohou být vakuově baleny nebo maskovány materiály, které snižují pravděpodobnost jejich zjištění při běžné kontrole.

2. **Samoobslužné výdejní boxy:** Samoobslužné výdejní systémy mohou snižovat osobní kontakt mezi odesílatelem a příjemcem a tím komplikovat identifikaci jednotlivých aktérů distribučního řetězce. Z hlediska vyšetřování tak představují další faktor, který může ztěžovat propojení zásilky s konkrétní osobou.

3. **Mrtvé schránky (Dead drops):** Tento model, v kriminologické literatuře popisovaný jako vysoce efektivní způsob eliminace osobního kontaktu, se v ČR adaptuje zejména ve velkých aglomeracích. Kurýr (kladmen) uloží látku na veřejně přístupné místo (např. pod lavičku, do dutiny stromu v parku) a kupující obdrží GPS souřadnice a fotografii místa.[13]

Z pohledu trestního práva je tento způsob distribuce problematický při prokazování subjektivní stránky trestného činu u kurýrů, kteří mohou tvrdit, že o obsahu zásilek nevěděli. Právě tato fáze je často nejslabším místem celého procesu. Tato skutečnost je významná zejména proto, že většina těchto případů se nakonec projeví ve fyzickém světě, kde dochází k předání, přepravě nebo zajištění nelegálních látek.

[13] ČT24. Policie odkryla prodej drog přes „darknet“. Pachatelé je posílali do celého světa. *ČT24* [online]. 22. 1. 2020 [cit. 2026-03-22]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/policie-odkryla-prodej-drog-pres-darknet-pachatele-je-posilali-do-celeho-sveta-53947

3 Právní rámec a možnosti odhalování obchodování s nelegálními látkami v online prostředí

Kriminalita na darknetu představuje specifický problém, protože se odehrává v digitálním prostředí a často přesahuje hranice jednotlivých států.

Právní úprava proto musí kombinovat klasické trestní právo s nástroji, které reagují na nové technologické podmínky.

3.1 Hmotněprávní aspekty drogové kriminality na darknetu

Základním právním předpisem je zákon č. 40/2009 Sb., Trestní zákoník. Klíčové je zejména ustanovení § 283, které upravuje nedovolenou výrobu a jiné nakládání s omamnými a psychotropními látkami.[14]

V případě darknetu je důležité, že:

- trestná činnost je často páchána prostřednictvím internetu
- může zasáhnout velké množství osob
- probíhá anonymně

Trestní zákoník proto počítá s přísnějším postihem v situaci, kdy je čin spáchán pomocí počítačové sítě.

Další relevantní ustanovení je § 287 (šíření toxikomanie), který se může uplatnit například u návodů nebo propagace drog na darknetových fórech.[15]

Jedním z obtížných momentů dokazování je prokázání subjektivní stránky jednání. V anonymizovaném online prostředí totiž nemusí být snadné doložit, že konkrétní osoba vystupovala vědomě, cíleně a s odpovídajícím úmyslem. V praxi to znamená, že i přes vysokou míru anonymity lze při správném postupu pachatele odhalit.

[14] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, § 283.
[15] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, § 287.

3.2 Procesněprávní rámec a specifika digitálního dokazování

Postup orgánů činných v trestním řízení se řídí trestním řádem (zákonem č. 141/1961 Sb.). V případě darknetu je ale práce s důkazy složitější než u běžné kriminality.[16]

Hlavním problémem je práce s digitální stopou neboli důkazem. Ten musí být zajištěn tak, aby bylo možné jeho použití u soudu.

V praxi to znamená například:

- **Zajišťování dat v počítačovém systému:** Podle § 78a Trestního řádu může policejní orgán vyzvat k vydání nebo uchování dat, která jsou důležitá pro trestní řízení.[17]
- **Admisibilita digitálních stop:** Aby bylo možné digitální důkaz u soudu použít, musí být zajištěn způsobem, který vyloučí pochybnosti o jeho původu a následných změnách. V praxi se proto využívají postupy umožňující zachovat původní obsah datového nosiče v podobě přesné forenzní kopie.
- **Domovní prohlídky a prohlídky jiných prostor:** Při vyšetřování kriminality spojené s darknetem se pozornost často soustředí na servery, počítače a mobilní zařízení podezřelých osob. Praktickou komplikací však bývá to, že uložená data mohou být šifrována, a jejich obsah tak nemusí být bez dalšího přístupný.

3.2.1 Operativně-pátrací prostředky (OPP)

Při odhalování trestné činnosti na darknetu hrají významnou roli i procesní nástroje upravené trestním řádem, zejména tehdy, když je nutné propojit online aktivitu s konkrétní zásilkou, osobou nebo komunikačním kanálem.

Mezi nejdůležitější patří:

[16] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: Sbírka zákonů České republiky, 1961.

[17] ŠÁMAL, Pavel a kol. Trestní řád: komentář. Praha: C. H. Beck, 2023, s. 1552.

1. **Předstíraný převod (§ 158c):** Umožňuje policistovi pod legendou zakoupit drogy na darknetovém tržišti. Tento úkon slouží k identifikaci distribuční cesty a získání vzorku látky.

2. **Sledování osob a věcí (§ 158d):** Zahrnuje monitorování pohybu zásilek s drogami v poštovním provozu.

3. **Zajištění a uchování dat v počítačovém systému (§ 7b):** Umožňuje orgánům činným v trestním řízení nařídit uchování dat důležitých pro trestní řízení, popřípadě znemožnit k nim přístup, aby nedošlo k jejich ztrátě, zničení nebo změně.[18]

U kryptoměn je důležité zajistit přístupové údaje (např. seed nebo privátní klíče). Bez nich není možné s prostředky nakládat.

3.2.2 Mezinárodní právo a Budapešťská úmluva

Kriminalita na darknetu má často mezinárodní charakter. Proto je důležitá spolupráce mezi státy.

Základním dokumentem je Úmluva o kyberkriminalitě (tzv. Budapešťská úmluva). Tu schválil Výbor ministrů Rady Evropy na svém 109. zasedání v listopadu roku 2001 v Budapešti a upravuje:

- spolupráci při vyšetřování
- zajišťování dat v zahraničí
- sdílení informací

Velkým problémem je otázka jurisdikce. Například:

- pachatel je v ČR
- server je v jiném státě
- droga je doručena do další země

V takovém případě je nutná koordinace mezi státy.[19]

---

[18] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 158c, § 158c a § 7b

[19] KOLOUCH, Jan, Pavel BAŠTA a kol. *CyberSecurity*. Praha: CZ.NIC, 2019. s 332-333

3.3 Mezinárodní spolupráce při potírání drogové kriminality

Pachatelé využívající digitální prostředí mají často technologický náskok před orgány činnými v trestním řízení. Tato forma kriminality má navíc zpravidla mezinárodní charakter, takže účinné odhalování závisí na úzké spolupráci mezi státy a jejich bezpečnostními institucemi. Bez mezinárodní spolupráce by bylo odhalování darknetové kriminality velmi obtížné.

Důležitou roli hrají:

- Europol
- Eurojust
- společné vyšetřovací týmy (JIT)

Tyto instituce umožňují sdílení informací a koordinaci zásahů ve více státech současně.

To znamená, že:

- data získaná v jedné zemi mohou být využita jinde
- zásahy probíhají současně, aby nedošlo ke zničení důkazů[20]

3.3.1 Mezinárodní spolupráce a Úmluva o kyberkriminalitě

Budapešťská úmluva byla přijata v roce 2001 a dosud je považována za klíčový mezinárodní dokument v této oblasti. Upravuje mimo jiné spolupráci při vyšetřování, zajišťování dat v zahraničí a sdílení informací mezi státy.[21]

V České republice funguje pro tyto účely kontaktní místo pod záštitou odboru informační kriminality Policejního prezidia, které zajišťuje komunikaci se zahraničními orgány.

[20] EUROPOL. *The trade in illicit drugs* [online]. The Hague: Europol [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/crime-areas/trade-in-illicit-drugs

[21] Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s., o Úmluvě o kyberkriminalitě.

Pro Českou republiku má Budapešťská úmluva význam zejména z hlediska mezinárodní právní spolupráce a rychlého zajišťování digitálních důkazů, které mohou být v online prostředí snadno odstraněny.[22]

Digitální prostředí má přeshraniční povahu a umožňuje velmi rychlé šíření informací i protiprávního obsahu. Z tohoto důvodu je nezbytné, aby existoval mezinárodní právní rámec, který stanoví základní pravidla spolupráce při potírání kyberkriminality.

„Rozvoj internetové trestní jurisdikce bude probíhat prostřednictvím dodatkových protokolů k Úmluvě, které postupně postihnou další konkrétní typy trestné činnosti či dokonce přestupků.“[23]

3.3.2 Česká legislativa v praxi

České právo se postupně přizpůsobuje tomu, že trestná činnost probíhá online. Použití internetu jako nástroje pro distribuci drog zvyšuje závažnost trestného činu, protože umožňuje oslovit velké množství lidí. Zároveň se řeší i obsah na fórech, například návody na výrobu drog. Ty mohou naplnit znaky trestného činu šíření toxikomanie. Využití počítačové sítě k distribuci drog prokazatelně zvyšuje společenskou škodlivost činu, neboť umožňuje zasáhnout řádově větší množství potenciálních uživatelů než klasický pouliční prodej.

Vedle distribuce je důležitý i § 287 Šíření toxikomanie. Na darknetových fórech se často vyskytují návody na domácí výrobu syntetických drog nebo rady, jak maskovat užívání látek. Pokud tato činnost směřuje k podněcování jiného ke zneužívání návykových látek, naplňuje znaky tohoto trestného činu i v digitální formě.[24]

3.3.3 Role Europolu a společné vyšetřovací týmy (JIT)

V praxi se jako velmi účinné ukázaly společné vyšetřovací týmy (JIT).

Jejich výhody:

---

[22] ČESKO. Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s., o Úmluvě o kyberkriminalitě. In: Sbírka mezinárodních smluv České republiky

[23] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP*. Brno: Computer Press, 2007, s. 16, cit. podle KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, 2016, s. 332

[24] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, § 287.

- rychlá výměna informací
- společné plánování zásahů
- koordinace mezi státy

Například při zásahu proti darknetovému tržišti může dojít k současnému zatýkání pachatelů ve více zemích.

4 Postupy bezpečnostních složek při odhalování nelegálních aktivit na darknetu

Odhalování trestné činnosti na darknetu vyžaduje změnu přístupu od tradičních reaktivních metod vyšetřování směrem k proaktivnímu monitoringu a pokročilé datové analýze.[25]

Bezpečnostní složky, v České republice primárně Národní protidrogová centrála (NPC), využívají kombinaci technických nástrojů a operativně-pátrací činnosti k narušení distribučních řetězců.

4.1 Monitoring skrytých služeb a dolování dat (Data Mining)

Prvotní fáze odhalování spočívá v kontinuálním sledování darknetových tržišť a diskusních fór. Vzhledem k obrovskému objemu dat je nezbytné využívat automatizované nástroje.

- **Web scraping a crawling:** bezpečnostní složky využívají specializované algoritmy k procházení onion domén a ke stahování informací o nabídkách, cenách, přezdívkách prodejců a jejich PGP (Pretty Good Privacy) klíčích. [26]

- **Analýza rizik a prevence**: včasná identifikace incidentů a hloubková analýza vzorců chování představují klíčové aspekty kybernetické bezpečnosti, neboť umožňují včasnou detekci nově vznikajících nelegálních platforem.[27]

- **Identifikace serverové infrastruktury**: snahou OČTR je lokalizovat fyzické servery, což je u sítě Tor komplikováno vícevrstvým šifrováním; vyšetřovatelé se proto zaměřují na chyby v konfiguraci serverů, které mohou odhalit jejich skutečnou IP adresu.[28]

[25] ABU AL-HAIJA, Qasem et al. SafeSurf Darknet 2025: A Novel Dataset for Darknet Traffic Detection and Analysis. Preprints, 2025, s. 1–2.
[26] SMEJKAL, Vladimír. Kybernetická kriminalita. Praha: Grada, 2019, s. 112.
[27] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019, s. 39-44.
[28] SMEJKAL, Vladimír. Kybernetická kriminalita. Praha: Grada, 2019, s. 118.

4.2 Finanční šetření a forenzní analýza blockchainu

Klíčovým článkem při odhalování prodejců je sledování finančních toků v kryptoměnách. Jednoduše řečeno, technologie sice pachatelům pomáhají skrýt identitu, ale zároveň vytvářejí nové stopy, které lze zpětně analyzovat. Ačkoliv jsou transakce pseudonymní, jejich historie je v blockchainu veřejně a trvale zapsána.[29]

- **Sledování transakcí**: Analytici využívají nástroje pro shlukování (clustering) adres, které umožňují propojit zdánlivě nesouvisející platby k jednomu subjektu.[30]

- **Průnik do anonymity**: Kritickým bodem je moment, kdy pachatel převádí kryptoměnu na fiatové peníze (např. CZK) skrze burzy nebo směnárny, které vyžadují identifikaci uživatele (KYC).[31]

- **Zajišťování virtuálních aktiv**: Zajištění kryptoměn jako výnosu z trestné činnosti vyžaduje specifické procesní postupy, zejména zajištění přístupových klíčů (tzv. seedů) v rámci domovních prohlídek, čímž se eliminuje riziko neoprávněného převodu prostředků pachatelem před jejich faktickým zajištěním ze strany policie.[32]

4.3 Operativní činnost a spolupráce s doručovacími službami

Protože darknetový obchod s drogami je ve své finální fázi závislý na fyzickém doručení zásilky, představuje poštovní a balíková přeprava jedno z nejzranitelnějších míst celého distribučního řetězce; orgány činné v trestním řízení

---

[29] CHAINALYSIS. *Why You Can't Trace Funds Through Services Using Blockchain Analysis*. Chainalysis, 9. 10. 2020 [online]. [cit. 30. 3. 2026]. Dostupné z:

[30] PAESANO, Francesco. *Cryptocurrencies and money laundering investigations*. Basel Institute on Governance, 2021 [online]. [cit. 27. 3. 2026]. Dostupné z: https://baselgovernance.org/sites/default/files/2021-08/QG%20crypto%20money%20laundering%20updated.pdf

[31] EUROPOL. *First Report on Encryption: Observations from Law Enforcement and Implications on EU Investigative Capability*. The Hague: Europol, 2024 [online]. [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf

[32] INDONESIA CORRUPTION WATCH. *Unravelling the Vulnerabilities of Abuse and Enforcement of Digital Currency related to Criminal Offences*. 2024 [online]. [cit. 30. 3. 2026]. Dostupné z: https://antikorupsi.org/sites/default/files/dokumen/ICW%20-%20Unravelling%20the%20Vulnerabilities%20of%20Abuse%20and%20Enforcement%20of%20Digital%20Currency%20related%20to%20Criminal%20Offencses%20%28EN%29.pdf

proto při odhalování podezřelých zásilek spolupracují i s dopravními a logistickými subjekty.

- **Sledování zásilek**: NPC úzce spolupracuje s Celní správou ČR a poštovními operátory při vytipovávání podezřelých balíků na základě profilování (např. země původu, způsobu balení).[33]

- **Nákupy pod legendou a monitorování darknetových tržišť**: Policisté pod legendou provádějí nákupy drog na darknetu, aby získali vzorky látek pro expertízu, a především adresy odesílatelů či digitální stopy v podobě kryptoměnových peněženek. Činní tak při odhalování prodejců drog na darknetu. Cílem těchto falešných nákupů je zisk důkazů a vystopování pachatele.[34]

- **Využití moderních technologií v terénu**: Při identifikaci pachatelů v terénu lze využívat také moderní technologické prostředky, zejména pokročilou videoanalytiku a biometrické nástroje, jakož i údaje o telekomunikačním provozu a lokalizaci, jsou-li v trestním řízení opatřeny zákonným způsobem.[35] [36]

4.4 Mezinárodní spolupráce a společné operace

Vzhledem ke globální povaze darknetu není národní úroveň vyšetřování sama o sobě zpravidla dostačující. Servery tržišť mohou být umístěny v jednom státě, jejich administrátoři působí z jiného území, prodejci odesílají zboží přes několik dalších zemí a zákazníci se nacházejí napříč různými jurisdikcemi. Vyšetřování této formy kriminality je proto závislé na intenzivní mezinárodní

[33] CELNÍ SPRÁVA ČR. *Výroční zpráva o činnosti Celní správy České republiky za rok 2024* [online]. 2025 [cit. 2026-03-27]. Dostupné z: https://celnisprava.gov.cz/cz/statistiky/Documents/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va%20o%20%C4%8Dinnosti%20Celn%C3%AD%20spr%C3%A1vy%20%C4%8Cesk%C3%A9%20republiky%20za%20rok%202024.pdf

[34] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2019* [online]. The Hague: Europol, 2019 [cit. 2026-03-27]. Dostupné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

[35] EUROPOL. *AI and policing* [online]. The Hague: Europol, 2024 [cit. 2026-03-30]. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

[36] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: Sbírka zákonů České republiky, 1961.

spolupráci, rychlé výměně informací a koordinovaném postupu policejních a justičních orgánů více států současně.[37]

- **Role Europolu a Interpolu**: Vzhledem k mezinárodní povaze darknetové kriminality je odhalování pachatelů podmíněno úzkou spoluprací mezi státy. Významnou roli v tomto směru sehrává zejména Europol, který poskytuje analytickou, koordinační a operační podporu při zásazích proti darknetovým tržištím a jejich administrátorům. V širším globálním měřítku pak obdobnou funkci plní také INTERPOL, jenž umožňuje výměnu informací a koordinaci přeshraničních policejních aktivit.[38] [39]

- **Společné vyšetřovací týmy (JITs)**: Významným nástrojem mezinárodní spolupráce jsou společné vyšetřovací týmy, které umožňují přímou a rychlou výměnu informací a důkazů mezi zapojenými státy. Jejich přínos spočívá zejména v tom, že snižují závislost na zdlouhavých formách mezinárodní právní pomoci, což je v digitálním prostředí mimořádně důležité, protože relevantní data mohou být během krátké doby smazána, přesunuta nebo zašifrována.[40]

- **Vytěžování zabavených serverů**: Podstatný význam má také analýza dat získaných při zajištění serverů a infrastruktury velkých darknetových tržišť. Takto získané informace, například údaje o zákaznících, prodejcích, objednávkách či komunikačních vazbách, mohou být následně předávány příslušným národním orgánům k dalšímu rozpracování a využity v navazujících vyšetřováních na místní úrovni.[41]

---

[37] EUROJUST. *Joint investigation teams* [online]. The Hague: Eurojust [cit. 2026-03-27]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams

[38] EUROPOL. *Europe-wide takedown hits longest-standing dark web drug market* [online]. 16. 6. 2025 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/europe-wide-takedown-hits-longest-standing-dark-web-drug-market

[39] INTERPOL. *What is INTERPOL?* [online]. [cit. 27. 3. 2026]. Dostupné z: https://www.interpol.int/Who-we-are/What-is-INTERPOL

[40] EUROJUST. *Joint investigation teams* [online]. [cit. 27. 3. 2026]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams

[41] EUROPOL. *270 arrested in global dark web crackdown targeting online drug and criminal networks* [online]. 22. 5. 2025 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/270-arrested-in-global-dark-web-crackdown-targeting-online-drug-and-criminal-networks

5 Historický vývoj a geneze nelegálního obchodu v kyberprostoru

Pochopení současných metod odhalování drogové kriminality na darknetu vyžaduje analýzu historického vývoje, který vedl k vytvoření současného anonymního ekosystému. Tento vývoj není jen o technologiích, ale také o tom, jak se postupně vyvíjí boj mezi pachateli a bezpečnostními složkami.[42]

Kořeny online obchodu s drogami sahají do raných fází internetové komunikace. Již v počátcích síťového propojení se objevily případy využití počítačové sítě ke zprostředkování nelegálních transakcí, i když tehdy ještě nešlo o prostředí založené na šifrování a anonymizačních technologiích.[43]

Rané fáze vývoje digitálního prostředí se vyznačovaly nižší mírou zabezpečení a menším důrazem na ochranu identity uživatelů.[44] Zásadní zlom nastal s rozvojem kryptografie, anonymizačních technologií a později sítě Tor, která vytvořila technický základ pro fungování skrytých služeb a anonymního online prostředí. Současně se tím prohluboval střet mezi ochranou soukromí a požadavkem státu na kontrolu a vyšetřování protiprávního jednání v kyberprostoru.[45]

5.1.1 Vývoj anonymizačních technologií: Projekt Tor

Zásadním technologickým milníkem pro vznik darknetu byl vývoj protokolu The Onion Routing (Tor). Paradoxem zůstává, že technologie, která dnes slouží k maskování nelegálních aktivit, byla původně vyvinuta americkým námořnictvem (U.S. Naval Research Laboratory) pro účely ochrany vládní komunikace.[46] [47]

---

[42] THE TOR PROJECT. History [online]. [cit. 31. 3. 2026]. Dostupné z: https://www.torproject.org/about/history

[43] THE GUARDIAN. Online highs are old as the net: the first e-commerce was a drugs deal [online]. 19. 4. 2013 [cit. 2. 3. 2026]. Dostupné z: https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal

[44] THE TOR PROJECT. *History* [online]. [cit. 2026-03-27]. Dostupné z: https://www.torproject.org/about/history/

[45] THE TOR PROJECT. *History* [online]. [cit. 2026-03-27]. Dostupné z: https://www.torproject.org/about/history/

[46] SMEJKAL, Vladimír. Kybernetická kriminalita. Praha: Grada, 2019, s. 112.

[47] STROUKAL, Dominik. Dark Web: Sex, drogy a bitcoiny. 2. vydání. Praha: Grada, 2020. s. 30-33

Veřejné zpřístupnění sítě Tor a jejího zdrojového kódu v roce 2002 přispělo k rozšíření anonymizačních technologií určených původně především k ochraně soukromí, svobody projevu a obraně proti cenzuře. Následný rozvoj skrytých služeb (hidden services, dnes onion services), které umožňují provoz služeb v síti Tor bez zveřejnění jejich skutečné síťové lokace, vytvořil technický základ pro vznik prostředí obtížně dostupného pro běžný dohled. Architektura Toru, založená na směrování komunikace přes více uzlů a na vrstveném šifrování, tak vedle legitimních účelů současně umožnila i vznik neregulovaných darknetových tržišť.[48] [49]

5.2 Silk Road a revoluce v distribučním modelu

Skutečný průlom v nelegálním obchodování s drogami přišel v únoru 2011, kdy Ross Ulbricht (pod pseudonymem Dread Pirate Roberts) spustil tržiště Silk Road. Silk Road jako první úspěšně integroval tři klíčové prvky:

1. **Anonymitu sítě Tor** pro skrytí identity serveru i uživatelů.
2. **Bitcoin** jako tehdy novou, decentralizovanou měnu pro anonymní platby.
3. **Systém hodnocení prodejců**, který vytvořil důvěru mezi anonymními subjekty.[50]

Tento model „Amazonu s drogami“ zcela změnil paradigma vyšetřování. Analýza platformy Silk Road prokázala, že nelegální trhy mohou v digitálním světě fungovat efektivněji než ty fyzické.

Pád Silk Roadu v roce 2013 a následné odsouzení jeho zakladatele k doživotnímu trestu ukázaly, že ani vysoká míra anonymity sama o sobě nevylučuje

[48] OR PROJECT. *History* [online]. [cit. 27. 3. 2026]. Dostupné z: https://www.torproject.org/about/history/

[49] DINGLEDINE, Roger, MATHEWSON, Nick a SYVERSON, Paul. *Tor: The Second-Generation Onion Router* [online]. 2004 [cit. 27. 3. 2026]. Dostupné z: https://freehaven.net/anonbib/cache/draft-tor-design-2004.pdf

[50] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2016, s. 49-50

odhalení pachatele, zejména pokud do vyšetřování vstoupí chyby v operativním chování a lidský faktor.[51] [52]

5.2.1 Éra fragmentace a operace Bayonet

Po zániku tržiště Silk Road nedošlo k útlumu darknetového prostředí, ale naopak k jeho další fragmentaci a technologickému zdokonalení. Na místo jednoho dominantního tržiště začaly vznikat nové platformy, mezi něž patřily například Silk Road 2.0, AlphaBay nebo Hansa Market. Tento vývoj současně vedl i k proměně policejních strategií, protože orgány činné v trestním řízení již neusilovaly pouze o vypnutí jednotlivých platforem, ale stále více se zaměřovaly také na infiltrační a analytické metody umožňující identifikaci širší sítě prodejců a zákazníků.[53] [54]

Za přelomovou lze v tomto směru označit operaci Bayonet realizovanou v roce 2017. V jejím rámci nizozemská policie skrytě převzala kontrolu nad tržištěm Hansa Market, které po určitou dobu ponechala v provozu pod svým dohledem. Cílem tohoto postupu nebylo pouze tržiště uzavřít, ale především monitorovat jeho provoz, zaznamenávat aktivitu uživatelů a získávat důkazy o prodejcích i zákaznících. Význam celé operace se ještě zvýšil v okamžiku, kdy po odstavení AlphaBay začala část uživatelů migrovat právě na Hansu, která byla již v té době pod kontrolou nizozemských orgánů. Tím se podařilo shromáždit rozsáhlé množství operativních a důkazních informací o fungování darknetového trhu.[55]

Aplikace této vyšetřovací metody ukazuje vysokou míru efektivity moderních infiltračních postupů v prostředí darknetu. Současně však otevírá i

---

[51] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2016, s. 49-50

[52] U.S. ATTORNEY'S OFFICE, SOUTHERN DISTRICT OF NEW YORK. *Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison* [online]. 2015-05-29 [cit. 2026-03-25]. Dostupné z: https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison

[53] EUROPEAN MONITORING CENTRE FOR DRUGS AND DRUG ADDICTION; EUROPOL. *Drugs and the darknet: perspectives for enforcement, research and policy* [online]. Luxembourg: Publications Office of the European Union, 2017 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

[54] UNITED STATES DEPARTMENT OF JUSTICE. *AlphaBay seizure* [online]. 2017 [cit. 20. 3. 2026]. Dostupné z: https://www.justice.gov/archives/opa/press-release/file/982831/dl?inline=

[55] EUROPOL. *Massive blow to criminal Dark Web activities after globally coordinated operation* [online]. 20. 7. 2017 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

významné právní a procesní otázky, zejména pokud jde o použitelnost a přípustnost takto získaných digitálních důkazů v trestním řízení, jejich autenticitu, zachování řetězce zajištění důkazu a přeshraniční spolupráci mezi státy. V mezinárodním prostředí je tato problematika obzvlášť citlivá, protože důkazní materiál bývá shromažďován v rámci operací přesahujících jednu jurisdikci a následně využíván v národních trestních řízeních.[56] [57]

5.2.2 Současnost: Decentralizace a anonymní měny

Historie nás učí, že každá úspěšná policejní operace vede k adaptaci pachatelů. V současnosti (výhledově do roku 2026) pozorujeme odklon od velkých centralizovaných tržišť směrem k menším, specializovaným fórům a přechod od Bitcoinu k anonymním kryptoměnám jako Monero. Současná kybernetická kriminalita je velmi flexibilní a dokáže se rychle přizpůsobit. [58]

Přesná definice pojmů je v oblasti kybernetické kriminality nezbytným předpokladem pro správnou právní kvalifikaci skutku a efektivní proces dokazování. Vzhledem k dynamickému vývoji technologií dochází často k terminologické nejednotnosti, kterou se tato kapitola snaží sjednotit s využitím relevantní odborné literatury.

5.2.3 Stručný výkladový slovník pojmů

- **Atribuce:** proces ztotožnění aktivity v kyberprostoru s konkrétní fyzickou osobou. V trestním řízení jde o nejnáročnější krok dokazování,

[56] YEBOAH-OFORI, Abel. *Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence* [online]. 2020 [cit. 27. 3. 2026]. Dostupné z: https://repository.uwl.ac.uk/8012/7/DigitalForensicsInvestigationJurisprudence-IssuesofAdmissibilityofDigitalEvidence.pdf

[57] KUCZYŃSKA, Hanna. *The ICC enters into the future: the digital-evidence revolution or evolution?* [online]. 2024 [cit. 27. 3. 2026]. Dostupné z: https://dialnet.unirioja.es/descarga/articulo/10189364.pdf

[58] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019, s. 140.

vyžadující řetězec nepřímých důkazů k potvrzení, že zařízení ovládala konkrétní osoba.

- **Digitální forenzní analýza:** odborné vyhledávání a zajišťování dat z elektronických zařízení.

- **Cibulové směrování (Onion Routing):** Technika anonymní komunikace sítě Tor, založená na vícenásobném šifrování dat, která procházejí přes řetězec uzlů, přičemž komunikace je rozdělena mezi více uzly a síť je navržena tak, aby zvyšovala anonymitu uživatele.[59]

- **Exit Node (Výstupní uzel):** Poslední bod sítě Tor, ve kterém data opouštějí šifrovaný tunel a vstupují do veřejného internetu. Je to jediné místo, kde lze monitorovat nešifrovaný obsah komunikace směřující k cíli.

- **Kryptoměnový mixér (Tumbler):** Služba určená k anonymizaci finančních toků na blockchainu tím, že promíchá vklady mnoha uživatelů a následně je vyplatí na nové, vzájemně nesouvisející adresy.

- **Tails OS:** Operační systém spouštěný z externího média, který veškerý provoz vynucuje přes síť Tor a po vypnutí nezanechává na pevném disku počítače žádné stopy.

- **Metadata:** Údaje o datech (např. čas odeslání, GPS souřadnice snímku, IP adresa). Mají často vyšší důkazní hodnotu než samotný obsah

[59] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. 6., doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, 2025, s. 210.

zprávy, protože jsou generovány automaticky vždy při zapnutí systému a jsou hůře falšovatelné.[60]

- **Multisignature (Multi-sig):** Bezpečnostní mechanismus digitálního podpisu vyžadující k autorizaci transakce v blockchainu souhlas více stran (např. kupujícího a administrátora tržiště).

- **OSINT (Open Source Intelligence):** Metodika získávání informací z otevřených a veřejně přístupných zdrojů. Slouží jako klíčová fáze operativního rozpracování před nasazením invazivnějších metod vyšetřování.

- **Předstíraný převod:** operativně-pátrací prostředek dle § 158c trestního řádu, spočívající v nákupu nelegální látky policistou pod legendou za účelem zajištění věcných a digitálních důkazů.[61]

- **Web Scraping:** Automatizované stahování dat z webových rozhraní (např. darknetových tržišť). OČTR tuto metodu využívá k hromadnému monitorování nabídek a profilů prodejců.

[60] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. 6., doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, 2025, s. 69.

[61] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 158c.

6 Kybernetický prostor a digitální prostředí

Kybernetický prostor představuje prostředí, ve kterém probíhá komunikace a práce s digitálními daty. Na rozdíl od fyzického světa nemá jasně dané hranice, což výrazně komplikuje jeho regulaci i vyšetřování trestné činnosti.[62]

V praxi je důležité rozlišovat mezi samotnými daty a fyzickou infrastrukturou, která jejich přenos umožňuje (např. servery nebo síťové prvky). Trestná činnost na darknetu se totiž odehrává především v digitální rovině, ale její důsledky se projevují ve světě reálném.

6.1 Digitální stopa a její specifika

Klíčovým pojmem pro kriminalistické zkoumání je digitální stopa. Digitální stopu lze definovat jako jakoukoli informaci v digitální podobě, ať už v uložené či přenášené formě, která má relevanci k vyšetřované události a může pomoci potvrdit nebo vyvrátit. Na rozdíl od stop materiálních (např. krevní skvrna) je digitální stopa:

- **Latentní:** vyžaduje technické prostředky k tomu, aby byla pro člověka čitelná.
- **Fragilní:** Snadno modifikovatelná nebo smazatelná bez zanechání viditelných stop po manipulaci.
- **Reprodukovatelná:** Lze vytvořit identickou kopii (bitovou kopii), která je z pohledu důkazní hodnoty rovnocenná originálu.

V kontextu darknetu jsou digitálními stopami zejména IP adresy (pokud nejsou maskovány), logy ze serverů, hlavičky PGP zpráv nebo záznamy v blockchainu.

6.1.1 Darknet a Overlay sítě

Darknet představuje specifické prostředí skrytých služeb a komunikačních platforem, které jsou provozovány nad běžnou internetovou infrastrukturou a zpravidla vyžadují speciální přístupové nástroje. Na rozdíl od hlubokého webu

[62] HRŮZA, Petr a kol. Kybernetická bezpečnost II. Brno, 2013, s. 9–10.

(Deep Web), jenž zahrnuje obsah obtížně dostupný běžnou navigací či standardním crawlingem, je darknet záměrně využíván pro anonymnější komunikaci a přístup. Z hlediska kybernetické bezpečnosti je významný tím, že ztěžuje identifikaci aktérů i analýzu jejich komunikace.[63] [64]

6.1.2 Asymetrické šifrování a PGP

Komunikace na darknetu je většinou zabezpečena pomocí asymetrického šifrování, konkrétně standardu PGP.

Princip je relativně jednoduchý:

- veřejný klíč slouží k zašifrování zprávy
- soukromý klíč k jejímu dešifrování[65]

Tím je zajištěno, že zprávu si může přečíst pouze její příjemce.

Pro vyšetřovatele to představuje zásadní problém. Pokud nemají k dispozici soukromý klíč, obsah komunikace zůstává nečitelný, i když se jim podaří získat samotný kryptogram nebo uložená data.[66]

6.1.3 Blockchain a kryptoměnová peněženka

Pro pochopení finančních toků je nutné definovat blockchain. Jde o distribuovanou a decentralizovanou databázi transakcí, která funguje jako transparentní účetní kniha.[67]

Přestože je blockchain veřejný (u Bitcoinu), identita uživatelů je skryta za adresy (pseudonymita). Kryptoměnová peněženka pak není místem, kde jsou

---

[63] ABU AL-HAIJA, Qasem et al. SafeSurf Darknet 2025: A Novel Dataset for Darknet Traffic Detection and Analysis. Preprints, 2025, s. 2.

[64] CHEN, Hsinchun. Dark Web: Exploring and Data Mining the Dark Side of the Web. New York: Springer, 2012, s. 46.

[65] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 6., doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, 2025. s. 136.

[66] HRŮZA, Petr a kol. Kybernetická bezpečnost II. Brno, 2013, s. 74–75.

[67] CHAINALYSIS. 2025 Crypto Crime Mid-Year Update [online]. New York: Chainalysis Inc., 2025 [cit. 2026-02-08]. Dostupné z WWW: https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/

uloženy peníze, ale nástrojem pro správu kryptografických klíčů, které umožňují manipulaci s jednotkami na blockchainu.[68]

6.1.4 Escrow a systémy vnitřní důvěry

Na darknetových tržištích fungují speciální mechanismy, které nahrazují běžné obchodní vztahy.

Jedním z nich je escrow, tedy úschova peněz. Princip spočívá v tom, že:

- kupující pošle peníze
- prostředky jsou dočasně zadrženy systémem
- prodejce je obdrží až po potvrzení doručení

Tento systém snižuje riziko podvodu a umožňuje fungování obchodu i mezi anonymními uživateli.

Zároveň ukazuje, že i nelegální prostředí si vytváří vlastní pravidla a formy „důvěry“.

V bezpečnostně-právní terminologii jde o nástroj eliminace rizika podvodu v kriminálním prostředí, který paradoxně zvyšuje efektivitu nelegálního obchodu. Existence těchto mechanismů ukazuje, že i nelegální online trhy si vytvářejí vlastní nástroje důvěry a koordinace, které zvyšují efektivitu obchodních vztahů mezi anonymními aktéry.[69]

[68] NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016, s. 40-60

[69] ELBAHRAWY, Abeer et al. Collective Dynamics of Dark Web Marketplaces. Scientific Reports, 2020, s. 2–3.

7 Metody odhalování a vyšetřování drogové kriminality na darknetu

Odhalování trestné činnosti v prostředí šifrovaných sítí vyžaduje změnu přístupu oproti tradičním metodám a interdisciplinární postup, který kombinuje pokročilou datovou analýzu s klasickými operativně-pátracími prostředky. Mechanismus asymetrického šifrování zajišťuje důvěrnost komunikace a při odpovídajícím použití klíčů i její autenticitu a integritu. V kyberprostoru pachatel usiluje o technologickou převahu založenou na anonymitě a obtížné dohledatelnosti, zatímco stát je při reakci omezen právním rámcem a reálnými technickými možnostmi.[70] [71]

7.1 Technické metody a digitální forenzní analýza

Prvním stupněm detekce je sběr dat přímo z darknetových tržišť. Tento proces, často označovaný jako web scraping, spočívá v automatizovaném stahování informací o nabízeném zboží, cenách, přezdívkách prodejců a jejich PGP klíčích. Při získávání dat z veřejně přístupných, byť technicky skrytých zdrojů v prostředí darknetu je nezbytné reflektovat specifické procesní aspekty, které podmiňují jejich následnou přípustnost a integritu při dokazování. Ale jejich následné využití jako důkazu v trestním řízení musí splňovat požadavky na integritu a autenticitu digitální stopy.

Klíčovou technickou metodou je analýza blockchainu. Přestože jsou kryptoměny někdy vnímány jako anonymní, u veřejných blockchainů, jako je Bitcoin, zůstává historie transakcí veřejně dohledatelná. Vyšetřovací a compliance nástroje využívají heuristiky pro propojování adres a identifikaci rizikových toků. Z praktického hlediska bývá významným bodem převod virtuálních aktiv do fiat měn prostřednictvím poskytovatelů služeb virtuálních aktiv, kteří podléhají identifikačním a kontrolním povinnostem typu KYC/CDD.[72]

---

[70] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. Právní problémy kybernetické bezpečnosti. Brno: Masarykova univerzita, 2016, s. 109 a 125.

[71] HRŮZA, Petr a kol. Kybernetická bezpečnost II. Brno, 2013, s. 62–75.

[72] FATF. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* [online]. Paris: FATF, 2021 [cit. 2026-03-27]. Dostupné z: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

7.2 Operativně-pátrací prostředky v digitálním prostředí

Vzhledem k technické náročnosti prolomení šifrování se těžiště vyšetřování často přesouvá k využití OPP dle hlavy deváté Trestního řádu.

- **Předstíraný převod (§ 158c tr. řádu):** Je v prostředí darknetových trhů významným prostředkem, protože umožňuje pod legendou provést kontrolovaný nákup a získat důkazy o distribučním mechanismu, odeslání zásilky i digitálních stopách spojených s platbou a komunikací.[73]
- **Sledování osob a věcí (§ 158d tr. řádu):** Může v kontextu darknetové kriminality zahrnovat sledování pohybu zásilek, návazných kontaktů a souvisejících digitálních stop. V technické rovině je přitom nutné rozlišovat mezi obsahem komunikace a provozními či lokalizačními údaji, jejichž získávání a hodnocení podléhá odlišným pravidlům a omezením.[74]

7.2.1 Využití institutu sledované zásilky a mezinárodní spolupráce

Pokud je identifikována podezřelá zásilka směřující z nebo do zahraničí, využívá se § 87b tr. řádu (Sledovaná zásilka). Namísto okamžitého zajištění je pohyb zásilky monitorován s cílem identifikovat konečného příjemce nebo odesílatele a rozkrýt celou distribuční síť. Tento postup vyžaduje úzkou součinnost s celní správou a provozovateli poštovních služeb.[75] [76]

Mezinárodní rozměr je v těchto případech klíčový. Operace proti darknetovým tržištím opakovaně ukázaly, že úspěch závisí na koordinaci zásahů ve více státech, sdílení informací a rychlém zajištění dat a souvisejících důkazů.[77]

---

[73] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 158c.

[74] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 158d.

[75] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 87b.

[76] ŠÁMAL, Pavel a kol. Trestní řád: komentář. Praha: C. H. Beck, 2023, s. 1553.

[77] EUROPOL. *International sting against dark web vendors leads to 179 arrests* [online]. 22. 9. 2020 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests

Operace jako DisrupTor nebo následné vyhodnocení dat po zániku Hydra Market ukázaly, že zásadní význam má rychlé mezinárodní sdílení informací a koordinované procesní zajištění digitálních důkazů.[78]

7.2.2 Limity dokazování a „lidský faktor“

I přes pokročilé technologie zůstává nejslabším článkem v řetězci pachatele lidský faktor. Řada úspěšných realizací vychází z kombinace technických chyb pachatele a následného precizního zajištění koncových zařízení při procesních úkonech.

[78] EUROPOL. *International sting against dark web vendors leads to 179 arrests* [online]. 2020-09-22 [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests

8 Moderní technologické trendy a výzvy v detekci

Boj proti drogové kriminalitě na darknetu již nespočívá pouze v reakci na jednotlivé skutky, ale stále více i v jejich včasné detekci. Současné pojetí kybernetické bezpečnosti proto zdůrazňuje význam identifikace anomálií v síťovém provozu a včasného rozpoznávání rizikových vzorců chování.

8.1 Využití OSINT a monitorování sociálních sítí

Ačkoliv se samotné transakce odehrávají v anonymizovaných prostředích, významná část komunikace, propagace a navazování kontaktů může probíhat i mimo hlavní tržiště. Metoda OSINT (Open Source Intelligence) je proto důležitým nástrojem pro sběr a třídění informací z otevřených nebo polootevřených zdrojů.[79]

Proces detekce může zahrnovat automatizované sledování klíčových slov, vyhodnocování dostupných metadat a korelaci identifikátorů napříč více platformami. Z právního hlediska však tyto poznatky slouží především jako operativní podnět a musí být následně doplněny procesně použitelnými důkazy získanými v souladu s trestním řádem.

8.2 Umělá inteligence a strojové učení v analýze trhu

S rostoucím objemem dat z darknetových prostředí nabývají na významu metody strojového učení a klasifikační algoritmy, které umožňují rozpoznávat anomálie, seskupovat podobné vzorce chování a podporovat analytické rozhodování.[80]

V praxi mohou být využívány pro třídění obsahu, analýzu komunikačních a transakčních vzorců nebo pro vyhodnocení rizikových profilů. Z toho plyne, že nejde pouze o technický problém, ale i o otázku správné interpretace dat a jejich využití v bezpečnostní a právní praxi.

---

[79] CHEN, Hsinchun. Dark Web: Exploring and Data Mining the Dark Side of the Web. New York: Springer, 2012, s. 341–344.

[80] ABU AL-HAIJA, Qasem et al. SafeSurf Darknet 2025: A Novel Dataset for Darknet Traffic Detection and Analysis. Preprints, 2025, s. 3–4 a 8–9.

8.3 Digitální forenzní analýza a „Zlatá hodina“ zajištění

Zajištění důkazního materiálu v digitální podobě představuje specifickou výzvu. Klíčovým aspektem digitální forenzní analýzy je zachování integrity digitální stopy v celém průběhu trestního řízení – od prvotního zajištění až po její předložení soudu.[81]

V prostředí darknetové kriminality může být kritická zejména analýza běžícího systému, protože některé relevantní údaje mohou být dostupné pouze po dobu jeho aktivního provozu. Pokud je zařízení zajištěno v běžícím stavu, může být nezbytné před jeho vypnutím provést úkony směřující k uchování například obsahu operační paměti. Ta může obsahovat přístupové údaje, klíče nebo jiné informace, které by po vypnutí zařízení již nebyly dostupné.[82]

8.4 Role agenta a předstíraného převodu

V moderním vyšetřování se využívá institut agenta podle § 158e tr. řádu i policisty vystupujícího pod legendou.[83]

Základním limitem je zákaz policejní provokace. V realitě to znamená že agent nesmí vyvolat trestnou činnost, která by jinak nevznikla, může však vstoupit do již probíhajícího jednání za účelem jeho dokumentace a rozkrytí širších souvislostí. V prostředí darknetu mohou podobné postupy směřovat i k dočasnému ovládnutí nebo monitorování komunikační platformy po zásahu proti jejím provozovatelům. Takový postup však vyvolává otázky jurisdikce, procesní použitelnosti důkazů a mezinárodní koordinace.

Na darknetu se tato činnost projevuje tzv. Převzetím administrace. Po zatčení administrátorů tržiště mohou OČTR (často v mezinárodní koordinaci) udržovat web v chodu pod svou kontrolou po omezenou dobu. Během této fáze sbírají adresy kupujících a prodejců, kteří se naivně domnívají, že platforma je stále

[81] POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015, s. 170-174

[82] POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015, s. 170-174

[83] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 158e.

bezpečná. Tento postup, ač efektivní, vyvolává řadu právních otázek ohledně jurisdikce a přípustnosti důkazů získaných v zahraničí.

8.4.1.1 Emerging Threats – Decentralizace a P2P sítě

Vedle dominantního postavení sítě Tor se v odborné literatuře objevují i další anonymizační a decentralizované technologie, například I2P nebo různé P2P architektury.[84]

Z bezpečnostního hlediska tyto technologie zvyšují odolnost prostředí vůči centralizovaným zásahům a ztěžují tradiční postupy založené na odstavení centrální infrastruktury. Vyšetřovací strategie se proto v takových případech více zaměřuje na infiltraci komunit, analýzu provozních a logistických vazeb a na propojení digitálních a fyzických stop.[85]

Jeden z příkladů představuje síť I2P (Invisible Internet Project). Na rozdíl od Toru, jenž používá cibulové směrování, I2P dává přednost tzv. „česnekovému směrování“ (garlic routing), jež shlukuje více zpráv do jednoho balíku a tím znemožňuje analyzovat provoz podle velikosti paketů. Další výzvou jsou decentralizovaná tržiště založená na P2P architektuře, kde absence centrálních serverů zásadně ztěžuje mezinárodní kooperaci při jejich odstavování. Inzeráty a hodnocení jsou distribuovány mezi všechny uživatele sítě, což činí tradiční metodu „Takedownu“ téměř neúčinnou a vyžaduje tak transformaci vyšetřovací strategie směrem k infiltraci komunit a analýze logistických řetězců ve fyzickém světě.[86]

---

[84] ABU AL-HAIJA, Qasem et al. SafeSurf Darknet 2025: A Novel Dataset for Darknet Traffic Detection and Analysis. Preprints, 2025, s. 2 a 15.

[85] CHEN, Hsinchun. Dark Web: Exploring and Data Mining the Dark Side of the Web. New York: Springer, 2012, s. 27 a 54.

[86] EUROPOL. *IOCTA 2025: Steal, deal and repeat* [online]. The Hague: Europol, 2025 [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/iocta-2025-steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

Praktická část

Případová studie: Operace Hydra, rozkrývání drogové kriminality v prostoru v České republice, diskuse a návrhy.

9 Charakteristika a geneze tržiště Hydra

Hydra představovala specifický fenomén, který se výrazně odlišoval od západních tržišť typu AlphaBay nebo Silk Road. Byla spuštěna v roce 2015 a postupně si vybudovala dominantní postavení na ruskojazyčném darknetovém trhu. Podle amerického ministerstva spravedlnosti v roce 2021 připadalo na Hydru přibližně 80 % všech darknet market-related cryptocurrency transactions s darknetovými tržišti.[87]

Hydra nebyla pouze inzertní platformou, ale komplexním digitálním ekosystémem, který zahrnoval i služby související se směnou kryptoměn a řešením sporů mezi uživateli. Z právního a bezpečnostního hlediska je významná tím, že vytvářela vlastní interní pravidla a mechanismy důvěry, čímž nahrazovala některé funkce běžného obchodního prostředí.[88][89]

9.1 Specifický modus operandi: Systém „kládů“

Na rozdíl od řady západních tržišť, která se ve větší míře opírala o poštovní doručování, rozvinula Hydra systém tzv. Dead drops (zakladki). V tomto modelu kurýr ukryje látku na veřejném místě, pořídí fotografii a doplní lokalizační údaje; kupující tyto informace získá až po zaplacení. Tento model významně omezuje přímý kontakt mezi prodávajícím a kupujícím a ztěžuje identifikaci distribučního řetězce.[90] [91]

---

[87] U.S. DEPARTMENT OF JUSTICE. *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace* [online]. 5. 4. 2022 [cit. 27. 3. 2026]. Dostupné z: https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

[88] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* [online]. 5. 4. 2022 [cit. 27. 3. 2026]. Dostupné z: https://home.treasury.gov/news/press-releases/jy0701

[89] GOONETILLEKE, Priyanka, KNORRE, Alex a KURIKSHA, Artem. Hydra: Lessons from the world's largest darknet market. Criminology & Public Policy. 2023, roč. 22, č. 4, s. 735–777 [online]. [cit. 31. 3. 2026]. Dostupné z: https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12647.

[90] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* [online]. 5. 4. 2022 [cit. 31. 3. 2026]. Dostupné z: https://home.treasury.gov/news/press-releases/jy0701

[91] GOONETILLEKE, Priyanka, KNORRE, Alex a KURIKSHA, Artem. Hydra: Lessons from the world's largest darknet market. Criminology & Public Policy. 2023, roč. 22, č. 4, s. 735–777 [online]. [cit. 31. 3. 2026]. Dostupné z: https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12647.

Proces probíhal následovně:

1. Prodejce najal kurýra (kladmena), který látku fyzicky ukryl na veřejném místě (např. v magnetickém pouzdře pod lavičkou nebo zakopanou v parku).

2. Kurýr pořídil fotografii místa, GPS souřadnice a nahrál je do systému Hydra.

3. Kupující po zaplacení obdržel tyto údaje a zásilku si vyzvedl bez jakéhokoliv kontaktu s jinou osobou.

Z pohledu trestního řízení představuje tento model komplikaci zejména při prokazování vědomé účasti jednotlivých článků distribučního řetězce. Významnou roli proto hraje zajištění digitálních stop z mobilních zařízení a navazujících datových zdrojů.

9.1.1 Průběh vyšetřování a identifikace serverové infrastruktury

Zlom v případu nastal v dubnu 2022, kdy německý Spolkový kriminální úřad (BKA) ve spolupráci s americkými orgány zasáhl proti infrastruktuře Hydry. Operace byla zaměřena nikoli na koncové uživatele, ale na technické zázemí tržiště. Německé orgány oznámily zabavení serverů provozovaných na území Německa a současně zajištění kryptoměn v hodnotě přibližně 23 milionů eur.[92] [93]

Z úhlu pohledu teorie kybernetické bezpečnosti je klíčové identifikovat fyzické umístění serverů, což je u sítě Tor extrémně náročné kvůli anonymizaci IP adres. Vyšetřovatelům se však podařilo odhalit, že Hydra využívala hostingové služby na území Německa. Ačkoliv provozovatel hostingu tvrdil, že neví, co na serverech běží, německá legislativa umožnila na základě důkazů o probíhající trestné činnosti servery zabavit.

---

[92] U.S. DEPARTMENT OF JUSTICE. *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace* [online]. 5. 4. 2022 [cit. 27. 3. 2026]. Dostupné z: https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

[93] EUROPOL. *288 dark web vendors arrested in major marketplace seizure* [online]. 2. 5. 2023 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

Při domovní prohlídce v datovém centru bylo zajištěno 17 serverů tvořících infrastrukturu Hydry a současně bylo zabaveno přibližně 23 milionů eur v bitcoinech. Zajištění serverové infrastruktury mělo zásadní význam pro následné získání a analýzu digitálních důkazů.

9.1.2 Analýza finančních toků a „Bitcoin Bank“

Hydra byla spojována i s interními mechanismy směny a praní výnosů z trestné činnosti. Americké úřady současně s tržištěm sankcionovaly i směnárnu Garantex, kterou označily za významný nástroj praní prostředků spojený s darknetem a ransomwarem. Z hlediska vyšetřování tak finanční analýza směřovala nejen k samotným transakcím v blockchainu, ale i k bodům, kde docházelo ke směně virtuálních aktiv za fiat měny nebo k jejich dalšímu pohybu přes regulované či poloregulované subjekty.[94] [95]

Vyšetřovatelé však využili pokročilou forenzní analýzu, která sledovala objemy transakcí směřující z peněženek Hydry do konkrétních směnáren s nízkou mírou regulace (např. Garantex). Tímto způsobem bylo možné identifikovat klíčové administrátory a „pračky peněz“, což vedlo k následnému uvalení sankcí na tyto subjekty ze strany ministerstva financí USA.

9.1.2.1 Právní a procesní dopady operace

Z právního hlediska operace Hydra potvrdila význam mezinárodní spolupráce při zajišťování serverů, kryptoměn a digitálních důkazů v různých jurisdikcích. Případ zároveň ukázal, že úspěch podobných zásahů nebývá založen na ‚prolomení‘ sítě Tor jako takové, ale spíše na kombinaci finančního šetření,

[94] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Russia-Based Hydra, World’s Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* [online]. 5. 4. 2022 [cit. 27. 3. 2026]. Dostupné z: https://home.treasury.gov/news/press-releases/jy0701

[95] OFAC. *Russia-related Designation; Cyber-related Designation* [online]. 5. 4. 2022 [cit. 28. 3. 2026]. Dostupné z: https://ofac.treasury.gov/recent-actions/20220405

mezinárodní právní pomoci a procesně správného zajištění technické infrastruktury.[96] [97]

Po odstavení serverů se na stránce Hydry objevilo oznámení o zabavení domény německou policií. To mělo i obrovský psychologický efekt, kdy došlo k rozpadu důvěry v anonymitu darknetu. Pohledem české kriminalistiky je tento případ relevantní jako precedens pro nakládání s digitálními stopami obrovského rozsahu, které musí být následně analyzovány a roztříděny pro potřeby jednotlivých národních států, kam směřovaly dílčí dodávky.[98]

9.2 Analýza operace SpecTor: Od infrastruktury k distribuční síti

Zatímco operace zaměřené na tržiště typu Hydra cílily především na eliminaci technického zázemí, operace SpecTor, realizovaná v roce 2023 pod koordinací Europolu a ve spolupráci s bezpečnostními složkami devíti států, ukázala schopnost orgánů činných v trestním řízení navázat na dříve zajištěná data a využít je k identifikaci prodejců i kupujících. Operace přímo navazovala na předchozí odstavení Monopoly Marketu a ukázala, že digitální důkazy získané při zásahu proti tržišti mohou sloužit jako základ pro následné procesní úkony vůči koncovým článkům distribučního řetězce.[99] [100]

---

[96] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* [online]. 5. 4. 2022 [cit. 27. 3. 2026]. Dostupné z: https://home.treasury.gov/news/press-releases/jy0701

[97] U.S. DEPARTMENT OF JUSTICE. *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace* [online]. 5. 4. 2022 [cit. 27. 3. 2026]. Dostupné z: https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

[98] EMCDDA/EUDA. Drugs and the darknet: perspectives for enforcement, research and policy [online]. Lisbon: EUDA, 2024 [cit. 2026-02-08]. Dostupné z WWW: https://www.euda.europa.eu/darknet_en

[99] EUROPOL. *288 dark web vendors arrested in major marketplace seizure* [online]. 2. 5. 2023 [cit. 27. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

[100] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2024* [online]. Luxembourg: Publications Office of the European Union, 2024 [cit. 27. 3. 2026]. Část „Operation Spector Legacy". Dostupné z: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

9.2.1 Metodika vytěžování dat ze zabavených platforem

Klíčovým aspektem operace SpecTor bylo využití informací získaných po předchozím zásahu proti tržišti Monopoly Market. V praxi se ukázalo, že zajištění serverové infrastruktury a navazujících datových souborů může vytvořit procesní základ pro rozsáhlý soubor následných úkonů, včetně domovních prohlídek a identifikace osob zapojených do prodeje a distribuce. Vyšetřování tohoto typu je založeno zejména na analýze transakčních dat, digitálních identifikátorů a dalších stop, které přetrvávají i po odstavení samotné platformy.

Z hlediska bezpečnostně-právní činnosti je operace SpecTor významná především tím, že vedla k zatčení 288 osob napříč devíti státy a k zajištění majetku a komodit ve značném rozsahu. Europol uvádí, že při operaci bylo zajištěno přibližně 50,8 milionu eur v hotovosti a kryptoměnách, 850 kilogramů drog a 117 střelných zbraní. Případ tak ukázal, že i po odstavení tržiště zůstávají digitální a transakční stopy využitelné pro následné vyšetřování.[101] [102]

9.2.1.1 Logistické aspekty a zneužívání poštovních služeb

Operace SpecTor současně ukázala rozsáhlé zneužívání legitimních poštovních a kurýrních služeb pro distribuci omamných látek. Z hlediska trestního řízení tak vzniká napětí mezi ochranou listovního tajemství a potřebou účinné detekce zásilek, které jsou využívány k nelegálnímu obchodu. Významnou roli zde hrají mezinárodní spolupráce, analýza rizikových profilů zásilek a koordinace mezi policejními orgány, celní správou a dalšími subjekty zapojenými do přepravního řetězce.

9.3 Analýza českých případů darknetových prodejců

Pro praktickou část je potřebné zasadit teoretické poznatky do českého prostředí. Česká republika nevystupuje pouze jako tranzitní území, ale v některých

---

[101] EUROPOL. *288 dark web vendors arrested in major marketplace seizure* [online]. 2. 5. 2023 [cit. 31. 3. 2026]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

[102] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2024* [online]. Luxembourg: Publications Office of the European Union, 2024 [cit. 31. 3. 2026]. Část „Operation Spector Legacy“. Dostupné z: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

případech také jako země původu a distribuce omamných a psychotropních látek nabízených prostřednictvím darknetových tržišť a internetových komunikačních platforem. Zprávy orgánů činných v trestním řízení i státního zastupitelství dlouhodobě upozorňují na to, že prodej drog probíhá prostřednictvím internetu, platby jsou realizovány ve virtuálních měnách a drogy jsou rozesílány poštovními zásilkami do České republiky i do zahraničí.[103] [104]

9.3.1 Operativní rozpracování českých prodejců

Typickým příkladem postupu Národní protidrogové centrály jsou případy, v nichž pachatelé z území České republiky nabízeli drogy prostřednictvím darknetových tržišť a následně je distribuovali poštovní cestou do tuzemska i do zahraničí. V těchto případech hraje významnou roli monitoring poštovního provozu a navazující institut sledované zásilky podle § 191 trestního řádu, který umožňuje kontrolované sledování pohybu zásilky až do okamžiku jejího převzetí a následné rozkrytí dalších článků distribučního řetězce.[105] [106]

9.3.2 Právní výzvy u českých soudů: Judikát NS ČR k digitální distribuci

Z právního hlediska je v českém prostředí podstatné, že distribuce omamných a psychotropních látek prostřednictvím počítačové sítě může zvyšovat společenskou škodlivost činu a komplikovat dokazování zejména ve vztahu k identitě pachatele, rozsahu distribuce a skutečně dosaženému výnosu. V případech darknetové kriminality soudy často pracují s kombinací nepřímých důkazů, digitálních stop, záznamů o komunikaci, dat z poštovního provozu a transakčních údajů získaných z virtuálních měn nebo zajištěných zařízení.[107]

---

[103] ČT24. *Policie odkryla prodej drog přes „darknet“. Pachatelé je posílali do celého světa* [online]. 22. 1. 2020 [cit. 25. 3. 2026]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/policie-odkryla-prodej-drog-pres-darknet-pachatele-je-posilali-do-celeho-sveta-53947

[104] POLICIE ČR. *Operace „AIRBUS“ a „KOMP“* [online]. 22. 1. 2020 [cit. 27. 3. 2026]. Dostupné z: https://policie.gov.cz/clanek/operace-airbus-a-komp.aspx

[105] POLICIE ČR. *Operace „AIRBUS“ a „KOMP“* [online]. 22. 1. 2020 [cit. 27. 3. 2026]. Dostupné z: https://policie.gov.cz/clanek/operace-airbus-a-komp.aspx

[106] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 191.

[107] NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ. *Zpráva o činnosti státního zastupitelství za rok 2021* [online]. Brno: Nejvyšší státní zastupitelství, 2022 [cit. 27. 3. 2026]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2022/07/Zo%C4%8C_2021-textov%C3%A1_%C4%8D%C3%A1st.pdf

Značným procesním problémem zůstává dokazování reálné výše zisku realizovaného v kryptoměnách. Pokud obviněný odmítne vydat přístup k peněžence, soudy v ČR musí vycházet z nepřímých důkazů – např. z evidence prodejů na zabaveném serveru darknetového tržiště, což je akceptovatelný důkaz, pokud je jeho autenticita potvrzena mezinárodní právní pomocí.[108]

9.3.2.1 Slabá místa českého systému a doporučení pro praxi

Analýza českých případů ukazuje, že významnou výzvou zůstává dostupnost specializovaných odborníků na digitální stopy, kryptoměnové transakce a práci s elektronickými důkazy, stejně jako rychlost mezinárodní právní pomoci ve vztahu k zahraničním poskytovatelům digitálních služeb. Z praktického hlediska je proto vhodné posilovat odborné kapacity v oblasti blockchainové analýzy, digitální forenzní podpory a efektivní mezinárodní spolupráce. Legislativní změny v oblasti tzv. Online prohlídek nebo rozšířené součinnosti poskytovatelů digitálních služeb však představují citlivou oblast, která by musela být posuzována s ohledem na ústavní limity, ochranu soukromí a procesní použitelnost takto získaných důkazů. [109]

9.4 Diskuse a návrhy opatření ke zvýšení efektivity odhalování

Tato kapitola shrnuje hlavní poznatky práce a formuluje doporučení, která podle mého názoru reagují na slabá místa současného systému odhalování drogové kriminality v digitálním prostředí. Z analýzy případů Hydra a SpecTor je patrné, že technický vývoj se v této oblasti posouvá velmi rychle a orgány činné v trestním řízení na něj musí reagovat nejen technicky, ale i organizačně a procesně. Ukazuje se, že samotná represivní reakce nestačí. Stejně důležitá je schopnost včas rozpoznat rizikové vzorce chování, rychle zajistit digitální důkazy a účinně spolupracovat se zahraničními partnery.

---

[108]UNODC. *World Drug Report 2024* [online]. Vienna: United Nations, 2024 [cit. 2026-03-15]. Dostupné z WWW: https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2024.html

[109] NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ. *Zpráva o činnosti státního zastupitelství za rok 2021* [online]. Brno: Nejvyšší státní zastupitelství, 2022 [cit. 27. 3. 2026]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2022/07/Zo%C4%8C_2021-textov%C3%A1_%C4%8D%C3%A1st.pdf

9.4.1 Legislativní doporučení a procesní výzvy (De lege ferenda)

Současný právní rámec České republiky obsahuje nástroje, které lze v prostředí darknetové kriminality využít. Přesto se v praxi ukazuje, že samotná existence těchto institutů neřeší všechny problémy, zejména pokud vyšetřování narazí na silné šifrování, decentralizované služby nebo zahraniční infrastrukturu.

Podle mého názoru by další vývoj neměl směřovat k jednoduchým a plošným zásahům do práv obviněných, ale spíše k přesně vymezeným procesním pravidlům pro nakládání s digitálními důkazy a pro včasné zajištění dat v běžícím systému. U úvah by proto měly být prioritou spíše větší právní jistota a rychlost procesních postupů než snaha o vytváření mimořádně invazivních oprávnění.

Za prakticky významné považuji také zjednodušení součinnosti mezi policejními orgány a provozovateli logistických či digitálních služeb, ovšem vždy při zachování soudní kontroly a přezkoumatelnosti zásahu. Pokud má být trestní řízení v této oblasti efektivní, musí být zároveň rychlé i procesně čisté.

9.4.2 Technická a organizační opatření

Z hlediska praxe považuji za důležitější než rozsáhlé legislativní změny především posílení odborného zázemí. Národní protidrogová centrála i další útvary podle mého názoru potřebují větší počet specialistů, kteří rozumějí blockchainové analýze, digitální forenzní práci a zajišťování elektronických důkazů. V řadě případů totiž není rozhodující schopnost „prolomit“ technologii jako takovou, ale schopnost správně vyhodnotit digitální stopy, které po sobě pachatel zanechá.

Stejně podstatné je i lepší propojení kriminalistické, technické a analytické složky vyšetřování. V prostředí darknetu se opakovaně ukazuje, že úspěch vychází ze spojení více menších poznatků – například údajů z poštovního provozu, digitálních identifikátorů, kryptoměnových transakcí a informací získaných z otevřených zdrojů. Samostatně by tyto stopy často nestačily, dohromady ale mohou vytvořit logický a procesně použitelný důkazní řetězec.

9.4.3 Prohloubení mezinárodní spolupráce

Přeshraniční povaha darknetu podle mého názoru zcela vylučuje představu, že by podobnou kriminalitu bylo možné účinně řešit jen na národní úrovni. Zásadní význam proto mají společné vyšetřovací týmy (JIT), které představují mezinárodní

nástroj spolupráce mezi justičními a policejními orgány více států. Bez rychlé výměny informací, koordinace zásahů a včasného zajištění serverů nebo datových stop by byly výsledky operací typu Hydra nebo SpecTor jen velmi omezené.

Do budoucna bych proto považoval za vhodné intenzivnější zapojení českých specialistů do společných mezinárodních týmů, a to nejen při samotných realizacích, ale i při analytické a přípravné fázi vyšetřování. Právě tam totiž často vzniká rozhodující výhoda oproti pachatelům.

9.4.4 Využití pokročilé analytiky a AI v detekční praxi

S rostoucím objemem dat už podle mého názoru není realistické spoléhat pouze na ruční analytickou práci. Pokročilá analytika, automatizované třídění dat a prvky strojového učení mohou významně pomoci při vyhledávání anomálií, při spojování souvisejících digitálních stop nebo při orientaci v rozsáhlých databázích získaných ze zabavených platforem.

Je ale důležité dodat, že tyto nástroje samy o sobě nenahrazují dokazování. Jejich role by měla být především podpůrná: pomáhat vytvářet vyšetřovací hypotézy, určit priority a zúžit okruh relevantních stop. Konečný význam takto získaných poznatků musí být vždy posuzován až v návaznosti na procesně řádně zajištěné důkazy.

9.4.5 Prohloubení součinnosti s logistickými řetězci v ČR

Za jedno z nejpraktičtějších míst zásahu stále považuji přechod z digitálního do fyzického světa. Právě okamžik předání nebo pohybu zásilky vytváří prostor, v němž se abstraktní anonymita internetu střetává s konkrétní fyzickou realitou. Z tohoto důvodu má podle mého názoru smysl prohlubovat součinnost s provozovateli logistických služeb, přepravci a dalšími subjekty, které se podílejí na doručovacím řetězci.

Taková spolupráce však musí mít jasná pravidla. Neměla by být postavena na plošném sledování všech uživatelů, ale na přesně vymezených postupech navázaných na důvodné podezření a soudně kontrolované úkony. Jen tak lze podle mého názoru skloubit efektivitu odhalování s ochranou soukromí a základních práv.

Závěr

Tato bakalářská práce si kladla za cíl zhodnotit, jaké jsou v současnosti možnosti odhalování nelegálního obchodu s látkami na darknetových tržištích, přičemž hlavní pozornost byla věnována postupům bezpečnostních složek v České republice. Během zpracování se potvrdilo, že prostředí darknetu je z pohledu vyšetřování velmi složité a nerovné – pachatelé zde běžně využívají technologie typu Tor, šifrování PGP a anonymní kryptoměny, což jim umožňuje účinně skrývat svoji identitu i finanční toky.

V teoretické části byly srozumitelně popsány technologické principy anonymizačních sítí a blockchainu, které hrají zásadní roli v digitální distribuci drog. Právní pohled ukázal, že ačkoliv české zákony na kyberkriminalitu reagují, v praxi narážejí vyšetřovatelé na konkrétní limity, zejména pokud jde o dokazování a určování příslušnosti v případě trestných činů spáchaných na dálku.

Analýza případových studií, jako byly operace Hydra a SpecTor, prokázala, že úspěšné odhalování těchto deliktů stojí na třech pilířích: mezinárodní koordinaci, hloubkové blockchainové analýze a využití tradičních operativně-pátracích prostředků v digitálním kontextu. Nejslabším článkem celého kriminálního řetězce paradoxně zůstává „lidský faktor“ – ať už v podobě chyb v operační bezpečnosti (OPSEC) na straně pachatelů nebo při fyzickém doručování zásilek v rámci logistického řetězce. Budoucnost úspěšné detekce v České republice proto neleží v prolomení šifer, ale v hloubkové analýze blockchainu a v úzké mezinárodní spolupráci při společných vyšetřovacích týmech (JIT). Navržená legislativní opatření, zejména v oblasti dešifrování dat, představují nezbytný krok k tomu, aby české právo dokázalo efektivně reagovat na výzvy digitální distribuce nelegálních látek v roce 2026.

Předkládaná bakalářská práce potvrdila, že odhalování drogové kriminality na darknetu je kontinuálním závodem v technologické vyspělosti mezi pachateli a státem. Analýza technologických principů sítě Tor a kryptoměn Monero či Bitcoin ukázala, že anonymita v kyberprostoru sice není absolutní, ale extrémně zvyšuje nároky na technické vybavení a odbornou připravenost OČTR.

Závěrem lze konstatovat, že i přes vysokou míru anonymity darknetu nejsou pachatelé nepostižitelní. Budoucnost vyšetřování leží v kombinaci klasické kriminalistiky s pokročilou datovou analytikou a umělou inteligencí. Navržená legislativní a technická opatření představují nezbytný krok k tomu, aby české bezpečnostní složky dokázaly udržet krok s neustále se vyvíjejícími trendy v oblasti online obchodu s návykovými látkami.

Seznam zdrojů

Literární zdroje

1. CHEN, Hsinchun. *Dark Web: Exploring and Data Mining the Dark Side of the Web*. New York: Springer, 2012. 451 s. ISBN 978-1-4614-1556-5.
2. GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
3. HRŮZA, Petr, Jaromír PITAŠ, Jaroslav ŠANDA a Bohumil BRECHTA. *Kybernetická bezpečnost II*. 1. vyd. Brno: Univerzita obrany, 2013. 100 s. ISBN 978-80-7231-931-2.
4. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 6., doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, 2025. 396 s.
5. KOLOUCH, Jan. *CyberCrime*. 1. vyd. Praha: CZ.NIC, 2016. 526 s. ISBN 978-80-88168-15-7.
6. KOLOUCH, Jan. *Kybernetická kriminalita: vybrané kapitoly*. Praha: Policejní akademie České republiky v Praze, 2020. 168 s. ISBN 978-80-7251-512-7.
7. KOLOUCH, Jan, Pavel BAŠTA a kol. *CyberSecurity*. 1. vyd. Praha: CZ.NIC, 2019. 556 s. ISBN 978-80-88168-31-7.
8. MARTIN, James. *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*. Basingstoke: Palgrave Macmillan, 2014. 256 s. ISBN 978-1-137-39904-5.
9. NARAYANAN, Arvind, Joseph BONNEAU, Edward FELTEN, Andrew MILLER a Steven GOLDFEDER. *Bitcoin and Cryptocurrency*

Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016. 336 s. ISBN 978-0-691-17169-2.

10. ORMSBY, Eileen. *The Darkest Web: Drugs, Death and Destroyed Lives ... the Inside Story of the Internet's Evil Twin*. Crows Nest: Allen & Unwin, 2021. 320 s. ISBN 9781760875626.
11. POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. 955 s. ISBN 978-80-7598-064-9.
12. POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, 2015. 253 s. ISBN 978-80-210-8073-7.
13. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vyd. Plzeň: Aleš Čeněk, 2019. 597 s. ISBN 978-80-7380-761-0.
14. STROUKAL, Dominik. *Dark Web: Sex, drogy a bitcoiny*. 1. vyd. Praha: Grada, 2020. 208 s. ISBN 978-80-271-2934-8.
15. ŠÁMAL, Pavel a kol. *Trestní řád: komentář*. 7. vyd. Praha: C. H. Beck, 2023. 4968 s. ISBN 978-80-7400-921-1.
16. ABU AL-HAIJA, Qasem, Mohammad J. OBAIDAT, Ibrahim A. AL-SYOUF, Yahea F. AWAWDEH a Anas E. MASA'DEH. *SafeSurf Darknet 2025: A Novel Dataset for Darknet Traffic Detection and Analysis*. *Preprints*, 2025. 17 s. DOI 10.20944/preprints202507.1926.v1.
17. ELBAHRAWY, Abeer, Laura ALESSANDRETTI, Leonid RUSNAC, Daniel GOLDSMITH, Alexander TEYTELBOYM a Andrea BARONCHELLI. *Collective dynamics of dark web marketplaces*. *Scientific Reports*. 2020, roč. 10, č. 1, čl. 18827.

Elektronické zdroje

1. ANYCOIN. *Bitcoin není anonymní a zločinci to dobře vědí* [online]. [cit. 2026-03-27]. Dostupné z: https://www.anycoin.cz/blog/blog-btc-anonymita?locale=cs_CZ
2. BASEL INSTITUTE ON GOVERNANCE. *Cryptocurrencies and money laundering investigations* [online]. 2021 [cit. 2026-03-27]. Dostupné z:

https://baselgovernance.org/sites/default/files/2021-08/QG%20crypto%20money%20laundering%20updated.pdf

3. CELNÍ SPRÁVA ČR. *Výroční zpráva o činnosti Celní správy České republiky za rok 2024* [online]. 2025 [cit. 2026-03-27]. Dostupné z: https://celnisprava.gov.cz/cz/statistiky/Documents/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va%20o%20%C4%8Dinnosti%20Celn%C3%AD%20spr%C3%A1vy%20%C4%8Cesk%C3%A9%20republiky%20za%20rok%202024.pdf
4. CHAINALYSIS. *2025 Crypto Crime Mid-Year Update* [online]. New York: Chainalysis Inc., 2025 [cit. 2026-02-08]. Dostupné z: https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/
5. CHAINALYSIS. *Why You Can't Trace Funds Through Services Using Blockchain Analysis* [online]. 2020-10-09 [cit. 2026-03-30]. Dostupné z: https://www.chainalysis.com/blog/blockchain-analysis-trace-through-service-exchange/
6. ČT24. *Policie odkryla prodej drog přes „darknet". Pachatelé je posílali do celého světa* [online]. 2020-01-22 [cit. 2026-03-25]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/policie-odkryla-prodej-drog-pres-darknet-pachatele-je-posilali-do-celeho-sveta-53947
7. DINGLEDINE, Roger, MATHEWSON, Nick a SYVERSON, Paul. Tor: The Second-Generation Onion Router [online]. 2004, s. 303–304 [cit. 27. 3. 2026]. Dostupné z: https://freehaven.net/anonbib/cache/draft-tor-design-2004.pdfEMCDDA a EUROPOL. *Drugs and the darknet: perspectives for enforcement, research and policy* [online]. Luxembourg: Publications Office of the European Union, 2017 [cit. 2026-03-27]. Dostupné z:

https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

8. EUDA. *European Drug Report 2025: Trends and Developments* [online]. Lisbon: EUDA, 2025 [cit. 2026-02-08]. Dostupné z: https://www.euda.europa.eu/publications/european-drug-report/2025
9. EUROJUST. *Joint investigation teams* [online]. The Hague: Eurojust [cit. 2026-03-27]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams
10. EUROPOL. *270 arrested in global dark web crackdown targeting online drug and criminal networks* [online]. 2025-05-22 [cit. 2026-03-27]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/270-arrested-in-global-dark-web-crackdown-targeting-online-drug-and-criminal-networks
11. EUROPOL. *288 dark web vendors arrested in major marketplace seizure* [online]. 2023-05-02 [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure
12. EUROPOL. *AI and policing* [online]. The Hague: Europol, 2024 [cit. 2026-03-30]. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing
13. EUROPOL. *EU Drug Markets: Drivers and Facilitators* [online]. The Hague: Europol, 2024 [cit. 2026-02-15]. Dostupné z: https://www.euda.europa.eu/news/2024/eu-drug-markets-drivers-and-facilitators-new-report-unveils-dynamics-illicit-drug-market_en
14. EUROPOL. *Europe-wide takedown hits longest-standing dark web drug market* [online]. 2025-06-16 [cit. 2026-03-27]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/europe-wide-takedown-hits-longest-standing-dark-web-drug-market
15. EUROPOL. *First Report on Encryption: Observations from Law Enforcement and Implications on EU Investigative Capability* [online]. The Hague: Europol, 2024 [cit. 2026-03-27]. Dostupné z:

https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf

16. EUROPOL. *International sting against dark web vendors leads to 179 arrests* [online]. 2020-09-22 [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests
17. EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2019* [online]. The Hague: Europol, 2019 [cit. 2026-03-27]. Dostupné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019
18. EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2024* [online]. Luxembourg: Publications Office of the European Union, 2024 [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
19. EUROPOL. *IOCTA 2025: Steal, deal and repeat – How cybercriminals trade and exploit your data* [online]. The Hague: Europol, 2025 [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/iocta-2025-steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data
20. EUROPOL. *Massive blow to criminal Dark Web activities after globally coordinated operation* [online]. 2017-07-20 [cit. 2026-03-27]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
21. EUROPOL. *The trade in illicit drugs* [online]. The Hague: Europol [cit. 2026-03-31]. Dostupné z: https://www.europol.europa.eu/crime-areas/trade-in-illicit-drugs
22. FATF. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* [online]. Paris: FATF, 2021 [cit. 2026-03-27]. Dostupné z: https://www.fatf-

gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

23. GLOBAL DRUG SURVEY. *GDS 2024 Key Findings* [online]. 2024 [cit. 2026-03-03]. Dostupné z: https://www.globaldrugsurvey.com/gds-2024/
24. GOONETILLEKE, Priyanka, Alex KNORRE a Artem KURIKSHA. *Hydra: Lessons from the world's largest darknet market* [online]. *Criminology & Public Policy*. 2023, roč. 22, č. 4, s. 735–777 [cit. 2026-03-31]. Dostupné z: https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12647
25. INDONESIA CORRUPTION WATCH. *Unravelling the Vulnerabilities of Abuse and Enforcement of Digital Currency related to Criminal Offences* [online]. 2024 [cit. 2026-03-30]. Dostupné z: https://antikorupsi.org/sites/default/files/dokumen/ICW%20-%20Unravelling%20the%20Vulnerabilities%20of%20Abuse%20and%20Enforcement%20of%20Digital%20Currency%20related%20to%20Criminal%20Offencses%20%28EN%29.pdf
26. INTERPOL. *INTERPOL Annual Report 2024* [online]. Lyon: Interpol, 2025 [cit. 2026-03-03]. Dostupné z: https://www.interpol.int/content/download/23674/file/Annual_Report%202024_EN.pdf
27. INTERPOL. *What is INTERPOL?* [online]. [cit. 2026-03-27]. Dostupné z: https://www.interpol.int/Who-we-are/What-is-INTERPOL
28. KUCZYŃSKA, Hanna. *The ICC enters into the future: the digital-evidence revolution or evolution?* [online]. 2024 [cit. 2026-03-27]. Dostupné z: https://dialnet.unirioja.es/descarga/articulo/10189364.pdf
29. NÁRODNÍ MONITOROVACÍ STŘEDISKO PRO DROGY A ZÁVISLOSTI. *Zpráva o drogách v České republice 2024* [online]. Praha: Úřad vlády České republiky, 2025 [cit. 2026-03-18]. Dostupné z: https://www.drogy-info.cz/publikace/vyrocni-zpravy/zprava-o-nelegalnich-drogach-v-ceske-republice-2024/
30. NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024* [online]. Brno: NÚKIB, 2025 [cit. 2026-03-10]. Dostupné z:

https://nukib.gov.cz/cs/kyberneticka-bezpecnost/zpravy-o-stavu-kyberneticke-bezpecnosti/

31. OFAC. *Russia-related Designation; Cyber-related Designation* [online]. 2022-04-05 [cit. 2026-03-28]. Dostupné z: https://ofac.treasury.gov/recent-actions/20220405
32. PAESANO, Francesco. *Cryptocurrencies and money laundering investigations* [online]. Basel Institute on Governance, 2021 [cit. 2026-03-27]. Dostupné z: https://baselgovernance.org/sites/default/files/2021-08/QG%20crypto%20money%20laundering%20updated.pdf
33. POLICIE ČR. *Národní protidrogová centrála: Výroční zpráva 2024* [online]. Praha: Policie ČR, 2025 [cit. 2026-03-10]. Dostupné z: https://policie.gov.cz/clanek/vyrocni-zpravy-kontroly.aspx
34. POLICIE ČR. *Operace „AIRBUS“ a „KOMP“* [online]. 2020-01-22 [cit. 2026-03-27]. Dostupné z: https://policie.gov.cz/clanek/operace-airbus-a-komp.aspx
35. THE TOR PROJECT. *History* [online]. [cit. 2026-03-27]. Dostupné z: https://www.torproject.org/about/history/
36. THE GUARDIAN. Online highs are old as the net: the first e-commerce was a drugs deal [online]. 19. 4. 2013 [cit. 2. 3. 2026]. Dostupné z: https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal
37. U.S. ATTORNEY'S OFFICE, SOUTHERN DISTRICT OF NEW YORK. *Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison* [online]. 2015-05-29 [cit. 2026-03-25]. Dostupné z: https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison
38. U.S. DEPARTMENT OF JUSTICE. *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace* [online]. 2022-04-05 [cit. 2026-03-27]. Dostupné z: https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace
39. U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling*

Virtual Currency Exchange Garantex [online]. 2022-04-05 [cit. 2026-03-27]. Dostupné z: https://home.treasury.gov/news/press-releases/jy0701

40. UNODC. *World Drug Report 2024* [online]. Vienna: United Nations, 2024 [cit. 2026-03-15]. Dostupné z: https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2024.html
41. UNODC. *World Drug Report 2025* [online]. Vienna: United Nations, 2025 [cit. 2026-03-15]. Dostupné z: https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2025.html
42. UNITED STATES DEPARTMENT OF JUSTICE. *AlphaBay seizure* [online]. 2017 [cit. 2026-03-20]. Dostupné z: https://www.justice.gov/archives/opa/press-release/file/982831/dl?inline=
43. YEBOAH-OFORI, Abel. *Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence* [online]. 2020 [cit. 2026-03-27]. Dostupné z: https://repository.uwl.ac.uk/8012/7/DigitalForensicsInvestigationJurisprudence-IssuesofAdmissibilityofDigitalEvidence.pdf

Legislativní dokumenty a judikatura

1. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
2. ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: Sbírka zákonů České republiky, 1961.
3. ČESKO. Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s., o Úmluvě o kyberkriminalitě. In: Sbírka mezinárodních smluv České republiky. 2013.
4. NEJVYŠŠÍ SOUD ČR. *Rozhodnutí zn. 7 Tdo 1047/2021*. Brno: NS ČR, 2021.

Seznam zkratek

- **CIA** – Confidentiality, Integrity, Availability
- **CDD** – Customer Due Diligence
- **DNM** – Darknet Market
- **JIT** – Joint Investigation Team
- **KYC** – Know Your Customer
- **NPC** – Národní protidrogová centrála
- **OČTŘ** – orgány činné v trestním řízení
- **OPP** – operativně-pátrací prostředky
- **OSINT** – Open Source Intelligence
- **P2P** – peer-to-peer
- **PGP** – Pretty Good Privacy
- **RAM** – Random Access Memory
- **UNODC** – United Nations Office on Drugs and Crime
- **VPN** – Virtual Private Network