Trestná činnost páchaná v kybernetickém prostoru s důrazem na virtuální měny

MICHAL ČERNÝ[1]

DOI http://dx.doi.org/10.37355/fvpk-2025/ZC-03

Úvod

V posledních letech jsme svědky dramatické digitalizace lidské činnosti, což s sebou přináší nejen řadu výhod, ale i nové hrozby. Kybernetický prostor se stal nejen místem sdílení informací a obchodních transakcí, ale také prostorem pro různorodou trestnou činnost. Mezi nejpalčivější problémy patří zneužívání virtuálních měn, které nabízejí anonymitu a rychlost transakcí. Tento článek se věnuje komplexní analýze trestné činnosti v kyberprostoru, přičemž klade důraz na roli virtuálních měn v těchto aktivitách.

1 Kybernetický prostor a patologické jevy v kyberprostoru

Kybernetický prostor je dynamický a komplexní soubor informačních a komunikačních technologií, který zahrnuje nejen fyzickou infrastrukturu, jako jsou servery, kabelové systémy a datové centra, ale také software, sítě, data a lidskou interakci. Definice kyberprostoru se v akademické literatuře liší, avšak společným jmenovatelem je digitální prostor, kde probíhá komunikace, transakce a ukládání informací.

Patologické jevy v kyberprostoru zahrnují širokou škálu negativních fenoménů, které mění charakter sociálních interakcí a představují hrozbu pro jednotlivce i společnost. Mezi těmito jevy lze jmenovat: cyber-enabled crime (ostatní kriminalita páchaná v kyberprostoru) a cyber-dependent crime (kriminalita přímo závislá na kybernetické trestné činnosti).

Zásadním fenoménem, který proměnil kriminální aktivity v kyberprostoru, je rozšířené využití virtuálních měn. Tyto decentralizované digitální systémy, jako je například Bitcoin či Monero, poskytují vysokou úroveň anonymizace transakcí, což z nich činí atraktivní nástroj pro pachatele trestné činnosti. Virtuální měny nejsou vázány na žádnou centrální autoritu a mohou být využity ke skrytí identity a původu finančních prostředků, což z nich činí ideálním nástrojem pro legalizaci výnosů z trestné činnosti.

---

1 *Michal Černý, Policie České republiky - Národní centrála proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování. Problematice virtuálních měn v bezpečnostní praxi se věnuje od roku 2018. V současné době je doktorandem na Českém vysokém učení technickém v Praze – Fakultě biomedicínského inženýrství.*

Významným rizikovým faktorem je globalizace kyberprostoru, která umožňuje působení pachatelů z různých jurisdikcí, což znesnadňuje jejich vystopování a následné trestní stíhání. V současnosti se stává nezbytností interdisciplinární přístup spojující technické, právní a sociologické disciplíny k efektivnímu zkoumání a potírání kriminality v kybernetickém prostoru.

2 Cyber-enabled crime

Cyber-enabled crime (ostatní kriminalita páchaná v kyberprostoru) představuje skupinu trestných činů, které existovaly i před nástupem digitálních technologií, ale jejich dopad a efektivita se díky internetu výrazně zvýšily. V této kategorii se typicky objevují tradiční formy kriminality, jako jsou podvody, vydírání, legalizace výnosů z trestné činnosti, obchod s lidmi nebo financování terorismu, které však využívají digitální nástroje a infrastrukturu ke svému provedení.

Internet a technologie umožňují těmto činům získat novou dimenzi. Pachatelé mohou působit anonymně, přeshraničně a s minimálními náklady. Virtuální měny v této souvislosti hrají zásadní roli, protože pachatelům poskytují možnost provádět finanční transakce mimo dohled tradičních bankovních systémů.

Podstatnou charakteristikou ostatní kriminality páchané v kyberprostoru je, že sice není vázána výlučně na digitální infrastrukturu, avšak právě tato infrastruktura umožňuje její masivní rozmach a ztěžuje detekci i vyšetřování. Kryptoměny zde vystupují jako prostředek ekonomického zajištění trestné činnosti, čímž napomáhají jejímu dlouhodobému udržení a škálování.

Z hlediska forenzní analýzy a trestního stíhání představují kryptoměny výzvu nejen kvůli anonymitě a decentralizaci, ale také kvůli existenci technologických nástrojů, které dále komplikují orgánům činným v trestním řízení trasování toků kriminálních transakcí virtuálních měn. Odpovědí na tyto výzvy musí být kombinace technologického výzkumu, legislativních nástrojů a mezinárodní spolupráce.

3 Cyber-dependent crime

Kriminalita přímo závislá na kybernetické trestné činnosti představuje specifickou kategorii trestné činnosti, která je zcela podmíněna existencí a funkčností informačních technologií a digitální infrastruktury. Tato kriminalita by bez kyberprostoru a informačních a komunikačních technologií nemohla existovat, neboť samotný mechanismus spáchání trestného činu závisí na využití počítačových systémů, sítí a dat.

Virtuální měny v rámci této kriminality slouží především jako nástroj odměňování a financování. Pachatelé často požadují platby za dešifrování dat nebo za nezveřejnění exfiltrovaných informací právě prostřednictvím kryptoměn, které jim zajišťují vysokou

míru anonymity. Například ransomware útoky jsou v naprosté většině případů spojeny s požadavky na platbu v Bitcoinech nebo jiných kryptoměnách, čímž dochází k propojení sofistikované digitální trestné činnosti s decentralizovaným finančním systémem.

Specifickým problémem je existence tzv. „ransomware-as-a-service" (RaaS), kdy rozličné hackerské skupiny nabízejí své nástroje jako službu jiným pachatelům (RaaS affiliates) za podíl na zisku, přičemž veškeré transakce probíhají ve virtuálních měnách. Tento model zločinu snižuje technickou bariéru pro vstup do kyberkriminality a výrazně rozšiřuje spektrum potenciálních útočníků na rozličné cíle, které nelze předem žádným způsobem predikovat.

Vyšetřování kriminality typu cyber-dependent je komplikováno globálním charakterem útoků, anonymitou aktérů a složitostí digitálních stop. Odpověď na tuto výzvu musí spočívat nejen v legislativních opatřeních, ale také ve vývoji sofistikovaných nástrojů pro digitální forenzní analýzu, včetně specializovaných nástrojů pro trasování toků kryptoměnových transakcí. Významnou roli hraje rovněž mezinárodní spolupráce a sdílení informací mezi bezpečnostními složkami napříč státy v celosvětovém rozsahu.

4 Zneužití virtuálních měn ze strany pachatelů trestné činnosti

Virtuální měny se v posledních letech staly klíčovým nástrojem v rukou pachatelů trestné činnosti v kyberprostoru. Jejich hlavní výhodou je relativní anonymita, globální dostupnost a absence centrálního dohledu. Tyto vlastnosti činí z kryptoměn ideální prostředek pro převod a skrytí výnosů z trestné činnosti, stejně jako pro financování různých nelegálních aktivit.

Zneužití virtuálních měn má několik základních forem, které se často kombinují a překrývají. V následujících podkapitolách bude rozvedena jejich struktura a mechanismy zneužívání.

4.1 Pašování hotovosti nebo jiných aktiv

Virtuální měny umožňují digitální převod hodnoty bez nutnosti fyzického přesunu tradiční fiat měny či aktiv. Pachatelé využívají kryptoměny k obcházení tradičních kontrol kapitálových toků a devizových pravidel. Zatímco dříve bylo nutné pašovat fyzickou hotovost, dnes stačí zaslat privátní klíč nebo QR kód prostřednictvím aplikace využívající šifrovanou komunikaci. Tento postup se využívá např. při daňových únicích, korupčních schématech nebo převodu výnosů z trestné činnosti do bezpečných jurisdikcí, aby se zastřel původ trestnou činností získaných finančních prostředků.

4.2 Využívání legálních obchodních struktur

Organizace zapojené do praní peněz stále častěji využívají legální podnikatelské subjekty k zakrytí původu kryptoměnových transakcí. Jde například o kryptoburzy, směnárny,

těžební společnosti nebo podniky přijímající kryptoměny jako platbu. Přes tyto subjekty lze relativně snadno konvertovat kryptoměny do fiat měn nebo je legalizovat v rámci běžných obchodních transakcí. Dalším známým příkladem je vkládání trestnou činností získaných financí do zisků z legálních obchodů podnikatelského subjektu, aby na první dojem působil jako legitimní zisk.

4.3 Využívání sítě profesionálních zprostředkovatelů služeb

V digitálním prostředí operuje síť tzv. „money mules",[2] off-chain směnárníků a zprostředkovatelů, kteří za provizi převádějí kryptoměny do jiných měn či systémů. Tito prostředníci často operují na pomezí legality, a jejich činnost je obtížně sledovatelná. Jejich služby se využívají například při multi-layeringu[3] v rámci praní peněz.

4.4 Nové platební metody

Vedle známých kryptoměn roste popularita anonymních a obtížně vysledovatelných měn jako Monero. Tyto měny implementují pokročilé techniky skrytí odesílatele, příjemce i částky (např. ring signatures, stealth adresy). Dále se objevují nové formy platebních platforem, včetně decentralizovaných směnáren (DEX) a DeFi protokolů,[4] které eliminují potřebu centralizované kontroly a podléhají menšímu regulačnímu dohledu z pohledu „know your customer" (KYC).[5]

4.5 Financování terorismu a extremismu

Virtuální měny se stávají nástrojem financování teroristických organizací a extremistických skupin. Anonymita a neregulovanost kryptoměnových transakcí umožňuje skrytý převod prostředků bez detekce tradičními finančními institucemi. Byly zaznamenány případy, kdy teroristické skupiny veřejně sdílely kryptoměnové adresy pro sběr darů či výkupného.

4.6 Podpora terorismu a extremismu

Kromě přímého financování slouží kryptoměny také k podpoře infrastruktury extremistických hnutí: nákupu serverů, domén, šíření propagandy či nákupu vybavení.

---

2 Money mules jsou jednotlivci, kteří vědomě či nevědomě přenášejí nebo převádějí nelegálně získané finanční prostředky jménem třetí strany. V kontextu kyberkriminality často figuruje jejich role při převodu kryptoměn nebo při konverzi digitálních aktiv do fiat měn, čímž napomáhají maskování původu prostředků.

3 Multi-layering je druhá fáze procesu praní peněz, jejímž cílem je zahlazení původu nelegálně získaných prostředků. Probíhá prostřednictvím komplexních, často přeshraničních finančních operací. Tímto způsobem dochází k rozptýlení digitální stopy a znesnadnění detekce ze strany orgánů činných v trestním řízení.

4 DeFi protokol (z angl. Decentralized Finance) označuje finanční aplikace postavené na blockchainu, které umožňují provádění služeb typu půjčky, směny, spoření nebo obchodování bez potřeby centrální autority (např. banky). Tyto protokoly často fungují pomocí chytrých smluv (smart contracts) a umožňují anonymní, neregulované finanční interakce.

5 KYC (z angl. Know Your Customer) je proces identifikace a ověření totožnosti klienta, který finanční instituce a poskytovatelé služeb používají v rámci opatření proti praní peněz (AML) a financování terorismu.

Tyto transakce jsou často maskovány jako běžné platby, případně probíhají přes směnárny bez náležité identifikace klientů (no KYC Exchange).

4.7 Obchodování se zbraněmi a CBRN materiálem

Na dark webu jsou běžně k dispozici zbraně, výbušniny a potenciálně i chemické, biologické, radiologické a jaderné (CBRN) materiály. Veškeré platby v tomto prostředí probíhají téměř výlučně prostřednictvím kryptoměn. Díky anonymitě transakcí je obtížné vystopovat nejen finanční toky, ale i zúčastněné strany.

4.8 Darkweb a služby typu "crime as a service"

Darkweb se stal hlavní platformou pro nabídku nelegálních služeb formou „zločinu jako služby" (CaaS). Patří sem nájemné kybernetické útoky, vývoj a prodej malware, prodej přístupových údajů, falešných dokladů nebo kompromitovaných platebních karet. Platby probíhají primárně v kryptoměnách, které umožňují provozovatelům trhů i zákazníkům zůstat v anonymitě. Platformy často implementují vlastní escrow systémy,[6] čímž se snaží zvýšit důvěryhodnost v rámci ilegálních transakcí.

Z uvedeného vyplývá, že virtuální měny nejsou pouze pasivním nástrojem, ale aktivním faktorem umožňujícím nové formy trestné činnosti, které by bez těchto technologií nebyly realizovatelné v takovém rozsahu, rychlosti a anonymitě.

5 Shrnutí celosvětových trendů trestné činnosti s využitím virtuálních měn

V poslední dekádě došlo k zásadní proměně v charakteru a rozsahu využívání virtuálních měn v rámci různých forem trestné činnosti. Analýza celosvětových trendů ukazuje, že kryptoměny již nejsou marginálním fenoménem v digitální ekonomice, ale staly se integrální součástí modu operandi řady kriminálních skupin.

V oblasti cyber-enabled crime je patrný nárůst podvodů spojených s investicemi do kryptoměn, zejména formou „pump and dump"[7] či „pig butchering".[8] Pachatelé rovněž

---

6 Escrow je bezpečnostní mechanismus, při němž třetí strana (tzv. escrow agent) dočasně drží finanční prostředky mezi kupujícím a prodávajícím, dokud nejsou splněny podmínky obchodu. V kontextu darkweb tržišť slouží escrow k ochraně proti podvodům – platba v kryptoměně je uvolněna prodejci až po potvrzení dodání zboží či služby kupujícím.

7 Pump and dump je manipulační schéma běžné na neregulovaných trzích, při němž skupina aktérů uměle navýší cenu určitého aktiva (např. kryptoměny) šířením falešných nebo zavádějících informací (pump), aby jej následně ve špičce prodala s vysokým ziskem (dump). Po prodeji cena dramaticky klesá a ztráty nesou neinformovaní investoři.

8 Pig butchering (doslova „porážka prasete") je sofistikovaná forma online podvodu, při níž pachatel dlouhodobě buduje důvěru s obětí prostřednictvím falešného vztahu (často romantického nebo obchodního) s cílem přimět ji k investování do fiktivních kryptoměnových projektů nebo platforem. Po

využívají kryptoměny k maskování převodů výnosů z tradičních podvodů, jako jsou podvody s veřejnými zakázkami či falešné fakturace.

V oblasti cyber-dependent crime je hlavním trendem zneužívání ransomwaru, který zaznamenal mimořádný nárůst po roce 2020. Podle analýz Europolu a dalších mezinárodních organizací je více než 90 % výkupného požadováno právě v kryptoměnách, často s využitím anonymních platforem a decentralizovaných burz. Dále se šíří koncept „ransomware-as-a-service", kde útočníci nakupují nebo pronajímají škodlivý kód za kryptoměny.

Na darkwebu dochází k trvalému rozvoji tržních struktur, včetně sofistikovaných tržišť s vysokou mírou reputačního hodnocení, zákaznické podpory a escrow služeb. Tato tržiště slouží nejen pro obchod s omamnými a psychotropními látkami, zbraněmi a padělky, ale i pro objednávky kybernetických útoků a šíření dětské pornografie. Dominantním platebním prostředkem zůstává Bitcoin, přičemž u citlivějších transakcí převažuje Monero nebo další privacy-coiny.[9]

Organizovaný zločin využívá kryptoměny jako standardní nástroj pro přesun prostředků napříč jurisdikcemi a jejich „praní" pomocí řetězců směnáren, mixérů a prostředníků. Zaznamenán byl nárůst využití decentralizovaných financí (DeFi) ke konverzím bez nutnosti identifikace, čímž se narušují tradiční AML mechanismy. Vysoce organizované skupiny rovněž provozují vlastní směnárny či těžební zařízení jako zástěrku pro legalizaci výnosů z trestné činnosti.

Celkově lze konstatovat, že globalizace trestné činnosti v kombinaci s neregulovanými kryptoměnovými technologiemi výrazně komplikuje úsilí v oblasti forenzní detekce, vymáhání práva i mezinárodní spolupráce. Vývoj ukazuje nutnost adaptace legislativních a technických opatření na dynamicky se měnící prostředí kybernetické kriminality.

6 Výhled do budoucích trendů trestné činnosti s využitím virtuálních měn

Predikce vývoje v oblasti trestné činnosti spojené s virtuálními měnami vychází z aktuálních trendů, technologického vývoje, platné legislativy a přijatých regulačních opatření. Předpokládá se další růst sofistikovanosti kybernetických útoků, zvýšené využívání anonymizačních technologií a adaptace organizovaného zločinu na nové decentralizované systémy.

nashromáždění vysoké částky od oběti dochází k náhlému přerušení kontaktu.

9 *Privacy-coin je označení pro kryptoměny navržené tak, aby maximalizovaly anonymitu uživatelů a skryly podrobnosti o transakcích.*

6.1 Sofistikovanost a profesionalizace zločinu

Modely jako „Ransomware-as-a-Service" (RaaS) budou nadále rozšiřovat škálu aktérů zapojených do kyberkriminality. Důraz bude kladen na cílení útoků na vysoce hodnotné cíle (high value targets), tedy na kritickou infrastrukturu, zdravotnická zařízení a významné podniky. Tyto cíle jsou atraktivní nejen z hlediska možného výkupného, ale také pro svůj společenský dopad.

6.2 Zvýšená implementace AI do trestné činnosti

Umělá inteligence bude zneužívána k obcházení bezpečnostních systémů, automatizaci podvodů a generování personalizovaných phishingových útoků. Systémy AML/KYC budou cíleně obcházeny např. deepfake videi či generovanou identitou. Nástup generativní AI a strojového učení bude zastávat významnou roli v oblasti vývoje nových forem malwaru a identifikace slabých míst systémů v rámci penetračního testování cíle před samotnou realizací kybernetického útoku. Virtuální měny přitom zůstanou primárním způsobem monetizace.

6.3 Adaptace nových mechanismů pro praní peněz a financování terorismu

Kriminální aktéři budou intenzivněji využívat cross-chain technologie,[10] blockchainové „bridge"[11] a další decentralizované služby, které znesnadňují sledování původu prostředků. Takové mechanismy podporují tzv. „chain hopping", kdy dochází k převodům virtuální měny mezi různými blockchainy.

6.4 Využívání privátních virtuálních měn a anonymizace v kyberprostoru

Kriminální aktéři se ve stále větší míře odklánějí od transparentních blockchainů směrem k privátním měnám, jako jsou Monero a další privacy-coiny. Tato preference je reakcí na zvýšenou efektivitu sledovacích nástrojů a analytických platforem používaných při forenzním zkoumání veřejných blockchainů.

---

10 Cross-chain technologie umožňují vzájemnou interoperabilitu mezi různými blockchainovými sítěmi, což umožňuje převádět digitální aktiva (např. kryptoměny nebo tokeny) z jednoho blockchainu na druhý. V kontextu praní peněz a financování terorismu tyto technologie napomáhají tzv. „chain hoppingu", tedy skrývání původu prostředků přes složité a obtížně sledovatelné transakční struktury napříč více blockchainy.

11 Blockchainové bridge (mosty mezi blockchainy) jsou technologická řešení umožňující převod digitálních aktiv nebo informací mezi různými blockchainovými sítěmi. Umožňují například „uzamčení" tokenu na jednom blockchainu a vytvoření jeho ekvivalentu na jiném. Z hlediska kriminality zvyšují složitost sledování finančních toků, neboť zprostředkovávají tzv. cross-chain transakce, které mohou být zneužity k zakrytí původu prostředků.

6.5 Nárůst využívání DeFi a decentralizovaných směnáren (DEX)

Vzhledem k obtížné regulovatelnosti DeFi protokolů a jejich anonymní povaze se očekává zvýšené využití těchto nástrojů k legalizaci výnosů z trestné činnosti a praní peněz. Vznikají nové modely využívající decentralizované úvěrové a investiční platformy bez identifikace uživatelů.

Výhled do budoucího směřování trestné činnosti za využití virtuálních měn tedy ukazuje na nutnost rychlé adaptace jak technických nástrojů, tak právního prostředí. Kybernetická kriminalita bude nadále představovat významnou bezpečnostní výzvu, v níž virtuální měny představují univerzální, anonymní a obtížně sledovatelný platební nástroj pro různé formy trestné činnosti.

Závěr

Trestná činnost v kybernetickém prostoru, a zejména její propojení s virtuálními měnami, představuje jednu z nejkomplexnějších a nejrychleji se vyvíjejících výzev současného právního a bezpečnostního prostředí. Jak bylo v jednotlivých kapitolách zmíněno, virtuální měny významně napomáhají efektivitě, škálovatelnosti a anonymitě různých forem kriminality, a to od tradičních forem organizované obecné a finanční kriminality, až po sofistikované cyber-dependent kybernetické útoky.

Vývoj v této oblasti ukazuje na stále hlubší technologickou vyspělost z řad jednotlivých pachatelů, jejich schopnost využívat decentralizované a anonymní finanční nástroje, ale i jejich adaptabilitu vůči regulatorním zásahům. Zároveň roste hrozba kombinace kybernetických útoků s prvky hybridního válčení, financování terorismu či šíření propagandy a dezinformací.

Z odborného hlediska je zřejmé, že bez koordinované mezinárodní spolupráce, standardizace technických a právních přístupů, zvyšování úrovně kybernetické gramotnosti a vývoje forenzních nástrojů pro forenzní analýzu blockchainu nebude možné efektivně čelit současným a především novým podobám kriminality. Významná bude také role finančních institucí, technologických firem a výzkumných pracovišť při tvorbě prediktivních modelů, detekčních algoritmů a strategií prevence.

Závěrem lze konstatovat, že kryptoměny jako takové nejsou v prvé řadě kriminálním nástrojem. Jejich potenciál je neutrální a závisí na kontextu využití. Hlavní výzvou nadcházejících let bude nalezení rovnováhy mezi technologickým pokrokem, ochranou soukromí a zajištěním bezpečnosti společnosti před dynamicky se vyvíjejícími hrozbami digitálního věku.

Literatura

Europol (2025), European Union Serious and Organised Crime Threat Assessment. https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

Chainalysis (2025), The Chainalysis 2025 Crypto Crime Report. https://go.chainalysis.com/2025-Crypto-Crime-Report.html

Elliptic (2024), Typologies Report 2024. https://www.elliptic.co/resources/elliptic-typologies-report-2024

Elliptic (2022), Elliptic Cross-Chain Report. https://www.elliptic.co/hubfs/Cross%20Chain%20Report%20exec.pdf

TRM Labs (2025), Crypto Crime Report. https://www.trmlabs.com/resources/reports/2025-crypto-crime-report

FBI (2023), IC3 – Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf