

# ZVÝŠENIE ODOLNOSTI SLOVENSKA VOČI HYBRIDNÝM HROZBÁM POMOCOU POSILNENIA KAPACÍT VEREJNEJ SPRÁVY

Kód projektu: 314011CDW7

Realizácia projektu v rámci operačného programu „Efektívna verejná správa“ financovaného z Európskeho sociálneho fondu

## **Kybernetický rozmer hybridných hrozieb vo vzťahu k Policačnému zboru. Multiinštitucionálna súčinnosť a spolupráca v oblasti predchádzania a eliminácie hybridných hrozieb.**

pplk. doc. RNDr. Tatiana Hajdúková, PhD.  
Katedra informatiky a manažmentu  
Akadémie Policačného zboru v Bratislave

## Štruktúra prednášky:

- Vymedzenie kybernetickej bezpečnosti
- Vybrané útoky v kyberpriestore vo vzťahu ku hybridným hrozbám
- Kybernetický rozmer hybridných hrozieb vo vzťahu k PZ  
Počítačová kriminalita, vyšetrovanie TČ, o ktorých sa dôkazy nachádzajú v elektronickej podobe.  
Boj proti legalizácii výnosov z TČ a financovaniu terorizmu.
- Riziká pôsobenia cez sociálne siete – TIK TOK.

Cieľom prednášky je zvýšiť povedomie o opatreniach v boji proti HH a poukázať na vybrané formy HH v kyberpriestore v súvislosti s činnosťami, ktoré vykonáva PZ SR.

# Kybernetický rozmer hybridných hrozieb vo vzťahu k Policajnému zboru

Poskytovanie elektronických služieb a štruktúra vlastníctva internetových médií umožňuje vo svojich službách a správach sledovať rôzne súkromné záujmy, záujmy iných štátov aj prostredníctvom nátlaku a donucovania.

- EP** v novembri 2022 aktualizoval právne predpisy EÚ s cieľom
- zlepšiť ochranu a posilniť investície do silnej KB základných služieb a kritickej infraštruktúry EÚ,
  - posilniť pravidlá platné v celej EÚ,
  - sprísňujú požiadavky na posudzovanie rizík a podávanie správ pre kritické subjekty v 11 základných odvetviach za účelom eliminácie kyberhrozieb.

# Kybernetický rozmer hybridných hrozieb vo vzťahu k Policajnému zboru

Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 – riadenia KB štátu – nastavenie procesov, postupov a cieľov v KP odrážajúcich dynamiku hrozieb v aktuálnej spoločnosti.

- Technické aspekty používania technológií,
- Netechnické aspekty používania technológií – dôveryhodnosť, používateľov dodávateľov a subdodávateľov.
- Dôvera v dodávateľa pozostáva
  - z konečnej podoby dodaného riešenia (kvalita)
  - z dôvery v podnikateľské, právne a politické prostredie, v ktorom sa dodávateľ pohybuje a ktoré na neho pôsobí (záujmy svojho štátu vz. záujmy svojich zákazníkov).



- Pred tým, ako ruské vojská vtrhli na územie Ukrajiny a tanky prešli hranicami, Moskva útočila aj v kybernetickom priestore.
- Výrazným znakom hybridných hrozieb je ich neobmedzená variabilita foriem realizácie, významnou mierou sa uskutočňujú v kybernetickom priestore a v ďalšom texte budú subsumované pod oblasť kybernetických hrozieb.

# Kybernetický rozmer hybridných hrozieb vo vzťahu k Policajnému zboru

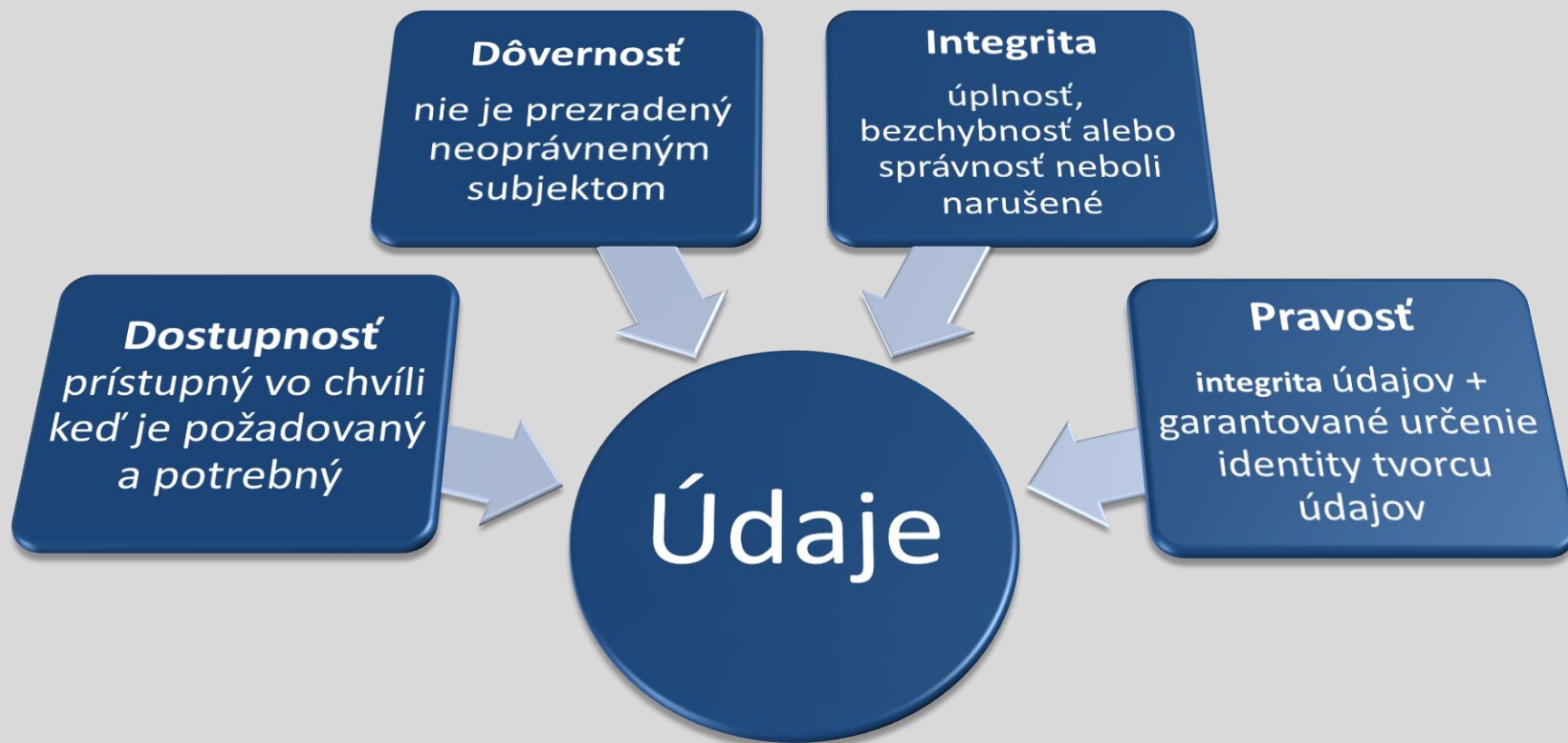


AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE

§3 ods. c) Z. 69/2018 Z. z. definuje kybernetický priestor (KP) ako globálny dynamický otvorený systém sietí a informačných systémov (IS), ktorý tvoria aktivované prvky KP, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.

Kybernetická bezpečnosť (KB) je v ods. g) def., ako „stav, v ktorom sú siete a IS schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje **dostupnosť, pravosť, integritu alebo dôvernú** uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a IS.





sieť internetových robotov, ktoré vykonávajú (aj bez vedomia používateľov PC) naprogramovanú obvykle škodlivú činnosť (spam, phishing, spear phishing, DOS, DDOS a podobne).

V Q1. 2021 FBI realizoval koordinovaný útok na infraštruktúru botnetu Emotet. NCKB SK-CERT získal od svojich partnerov stovky IP adries indikujúcich aktivitu Emotet botnetu v IP priestore SR, na základe ktorých realizoval koordinované odstraňovanie tohto obsahu, čo prispelo k zníženiu počtu zariadení ovládaných Emotetom v slovenskom KP. Popri botnete Emotet bolo adresne riešené botnety TrickBot, QuakBot, MERIS botnet, Conficker a 2 inštancie neznámeho botnetu.

Príklad multiinštitucionálnej súčinnosti a spolupráce v oblasti predchádzaní a eliminácii kybernetických hrozieb.



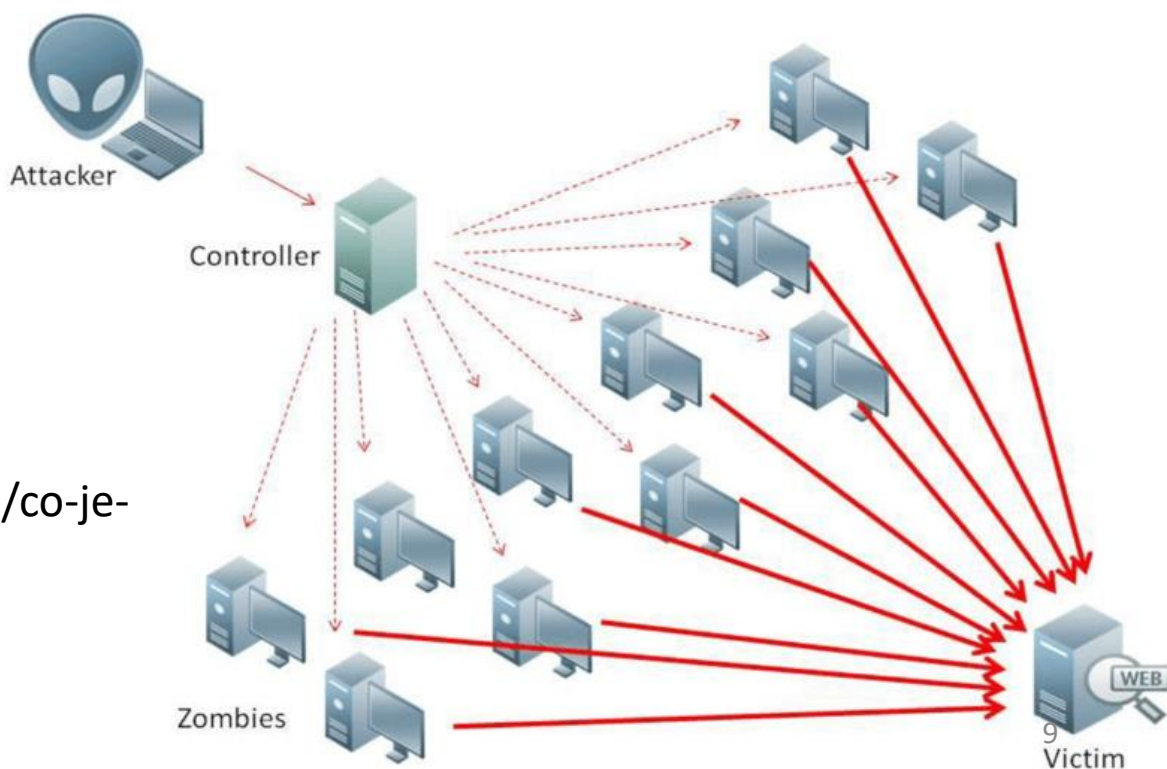
Zdroj obrázka:  
<https://www.istockphoto.com/>

Zdroj Správa o KB v SR 2021 NCKB SK-CERT



# Prevádzkový výpadok, DOS, DDOS

- zahltenie internetových služieb alebo webových stránok požiadavkami, ktoré smerujú k ich pádu, nefunkčnosti alebo nedostupnosti systému pre ostatných užívateľov, a to útokom z mnohých vektorov súčasne.
- Podvratná činnosť za účelom vynucovania vlastných cieľov.



Zdroj obrázka:

<https://cs.safetydetectives.com/blog/co-je-ddos-utok-a-jak-mu-zabranit/>



Operačný program  
**Efektívna  
verejná správa**

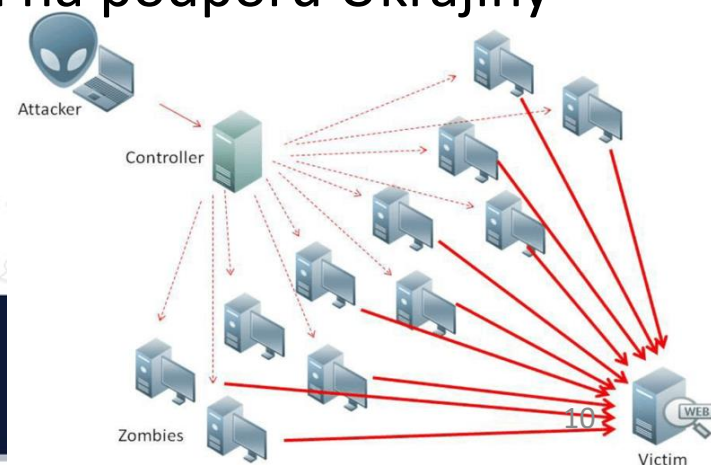


E  
E

# Prevádzkový výpadok, DOS, DDOS

- CSIRT.SK monitoroval niekoľko útokov typu DDoS na webové stránky viacerých štátnych organizácií MV SR ([www.minv.sk](http://www.minv.sk)), MO SR ([www.mosr.sk](http://www.mosr.sk)), MZVaEZ SR ([www.mzv.sk](http://www.mzv.sk), [foreign.gov.sk](http://foreign.gov.sk)), NR SR ([www.nrsr.sk](http://www.nrsr.sk)), Ústavný súd SR ([www.ustavnysud.sk](http://www.ustavnysud.sk)). Zasiahnuté boli aj weby bankového sektora (NBS, Exim banka a J&T banka) a ŽSR ([www.zsr.sk](http://www.zsr.sk)). Útoky boli vedené proruskými skupinami NoName057(16), Anonymous Russia a Killnet. Dané organizácie sa podľa vyjadrení skupín na ich telegramových kanáloch stali terčom útokov kvôli rozhodnutiu Slovenska poskytnúť ukrajinskej armáde stíhačky MIG 29 a všeobecne kvôli aktivitám na podporu Ukrajiny voči ruskej agresii.

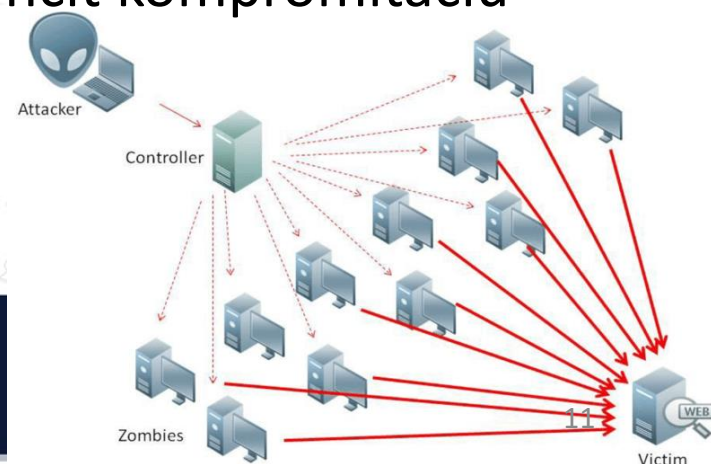
Zdroj: mesačná správa CSIRT SK – marec 2023



# Prevádzkový výpadok, DOS, DDOS

- V súvislosti s vojnou na Ukrajine sa v slovenskom KP vyskytli **výzvy na distribuované útoky na webové stránky** v Rusku a to pomocou jednoduchého webového odkazu, ktorý si “záujemca” má nechať otvorený v prehliadači. Vykonávaním distribuovaného útoku (napr. voči webovým stránkam v Rusku) **poskytujete príležitosť** na strane cieľa využiť informácie o zdroji útoku. Následne **môže byť vaše zariadenie kompromitované** a využívané na podobné DDoS útoky, len na iné ciele (napríklad na Ukrajinu alebo na Slovensku). Špeciálne upozornenie platí pre zamestnancov vo verejnom sektore, ktorí môžu takýmito činnosťami uľahčiť kompromitáciu ich pracovných zariadení. Zdroj: NBÚ SR

Zdroj obrázka: <https://cs.safetydetectives.com/blog/co-je-ddos-utok-a-jak-mu-zabranit/>





# Ransomvérový útok

Podvratná činnosť za účelom vynucovania vlastných, obvykle finančných ziskov.

Najväčšie problémy pri riešení ransomvérových incidentov v SR v roku 2021 (ISVS, Energetika) boli nedostatočné zálohovanie dát obetí, nedostatočná segmentácia vnútornej siete a veľké množstvo služieb dostupných z internetu.

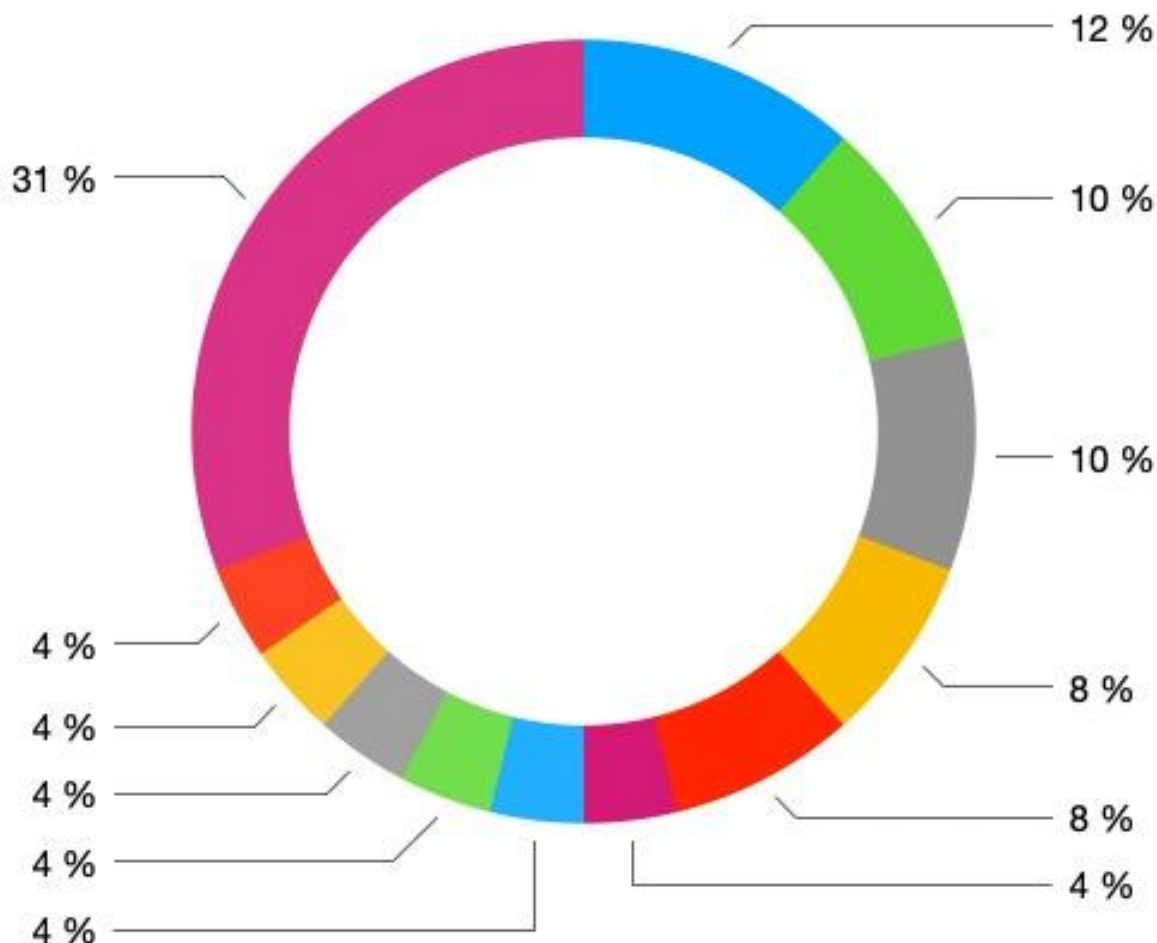


Zdroj obrázka: <https://www.istockphoto.com/>

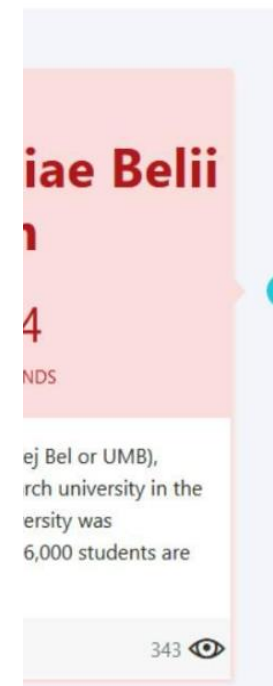
Zdroj Správa o KB v SR 2021 NCKB SK-CERT



- Vzdelávanie
- IT
- Právne firmy
- Zdravotníctvo
- Stavebníctvo
- Maloobchod
- Výroba
- Energetika
- Doprava
- Finančné služby
- Výroba
- Ostatných 16 kategórií



Prestali fungovať  
Prestala fungovať  
zo serverov Univerzity...



- Ovplyvňovanie verejnej mienky prostredníctvom rozvracania internetových diskusií, blogov, online platforiem, sociálnych sietí platenými trollmi (trollia farma, továreň). Snahou je vnášať medzi obyvateľov pocit strachu a neistoty, podporiť trhliny v spoločnosti.
- Komunikácia cez anonymné alebo fake-ovo vytvorené účty

- **Dôvody**

Osobné, vybiť frustráciu,  
zaujať, získať pozornosť,

Politické obvykle koordinovaná činnosť viacerých trollov,  
ktorý spoločne očierňujú konkrétnu politickú stranu alebo  
politika.

Trolling je špecifikom Ruskej hybridnej vojny.

je kombinácia aktivizmu a škodlivého hackera na demonštrovanie občianskej neposlušnosti.

- **Pohnútky** z protivládnych motívov, korporátnych krívd alebo sociálnej nespravodlivosti.
- **Ciele dosahujú** odhaľovaním a únikom údajov spojených s tými, ktorých obviňujú z neprávosti a degradujú a narušajú ich siete.
- **Nástroje** od prenajímateľných a jednoduchých až po sofistikované a pokročilé.
- **„úľové zmýšľanie“** ich aktivita je viac reakčná, sociálna a podporná ako plánovaná a organizovaná. Sú schopní spolupracovať, reagovať na udalosť a rozširovať informácie v priebehu niekoľkých hodín.
- **Dopady** od znepokojených občanov až po hrozbu pre štát v podobe tzv. vlasteneckého hacktivizmu.

# Riadenie rizík v kyberpriestore pri činnostiach príslušníkov PZ

Riadenie KB je zabezpečovanie ochrany informačných aktív vo virtuálnom priestore systematickým analyzovaním vplyvov, nastavovaním procesov, postupov a cieľov. Úspech v kolektívnej bezpečnosti je predovšetkým spoločná súhra a nastavenie mechanizmov správy KP.

- **aktualizácie** softvéru, firmvéru a všetkých systémov a služieb, predovšetkým bezpečnostnými záplatami.
- účinnosť **zálohovacieho manažmentu**, aktualizované zálohovacie procedúry,
- **viacfaktorová autentifikácia** (aj e-mailové služby a VPN služby). Používať autentifikačné spôsoby odolné voči sociálnemu inžinierstvu (napr. fyzické tokeny),



# Riadenie rizík v kyberpriestore pri činnostiach príslušníkov PZ

- Aktualizovaný **manažment prístupov** (odstrániť všetky staré a nepoužívané kontá, obmedzovať prístupy jednotlivých používateľov.
- **politika hesiel** (zákaz používať rovnaké heslá na rôzne služby, používanie silných hesiel alebo heslových fráz.
- **Nenavštevovať** nebezpečné, podozrivé alebo falošné webové lokality,
- S podozrením na akýkoľvek výskyt ransomwéru alebo iný kybernetický bezpečnostný incident sa okamžite obrátiť na **lokálneho IT správcu** a na kontakt Bezpečnostného a monitorovacieho centra MV SR **incident@minv.sk**.

# Kybernetický rozmer hybridných hrozieb vo vzťahu k Policajnému zboru



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE

## Národná centrála osobitných druhov kriminality

Odbor  
finančného  
vyšetovania

Odbor  
počítačovej  
kriminality

Odbor odhaľovania  
nebezpečných  
materiálov a  
environmentálnej  
kriminality

Oddelenie  
cieľového  
pátrania

Oddelenie  
podpory  
pátrania



Operačný program  
**Efektívna  
verejná správa**



**Európska únia**  
Európsky sociálny fond



# Vyšetrovanie TČ, o ktorých sa dôkazy nachádzajú v elektronickej podobe

- Nové technológie = nové spôsoby páchania tzv. „klasických“ TČ (krádež, podvod, vydieranie, ohováranie, nebezpečné prenasledovanie, rozširovanie nepravdivých informácií, nepravdivých údajov, poplašných správ. ) v kyberpriestore.
- TČ na objednávku (Crime as a Service) s väčším dopadom na spoločnosť.
- Z hľadiska vývoja kriminality v SR sa pri objasňovaní TČ v kyberpriestore zvyšuje potreba zabezpečiť
  - ☐ údaje komunikujúcich strán,
  - ☐ údaje z uskutočnenej telekomunikačnej prevádzky,
  - ☐ počítačové údaje uložené v počítačovom systéme,
  - ☐ údaje prostredníctvom počítačového systému len prenášané.

# Vyšetrovanie TČ, o ktorých sa dôkazy nachádzajú v elektronickej podobe



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE

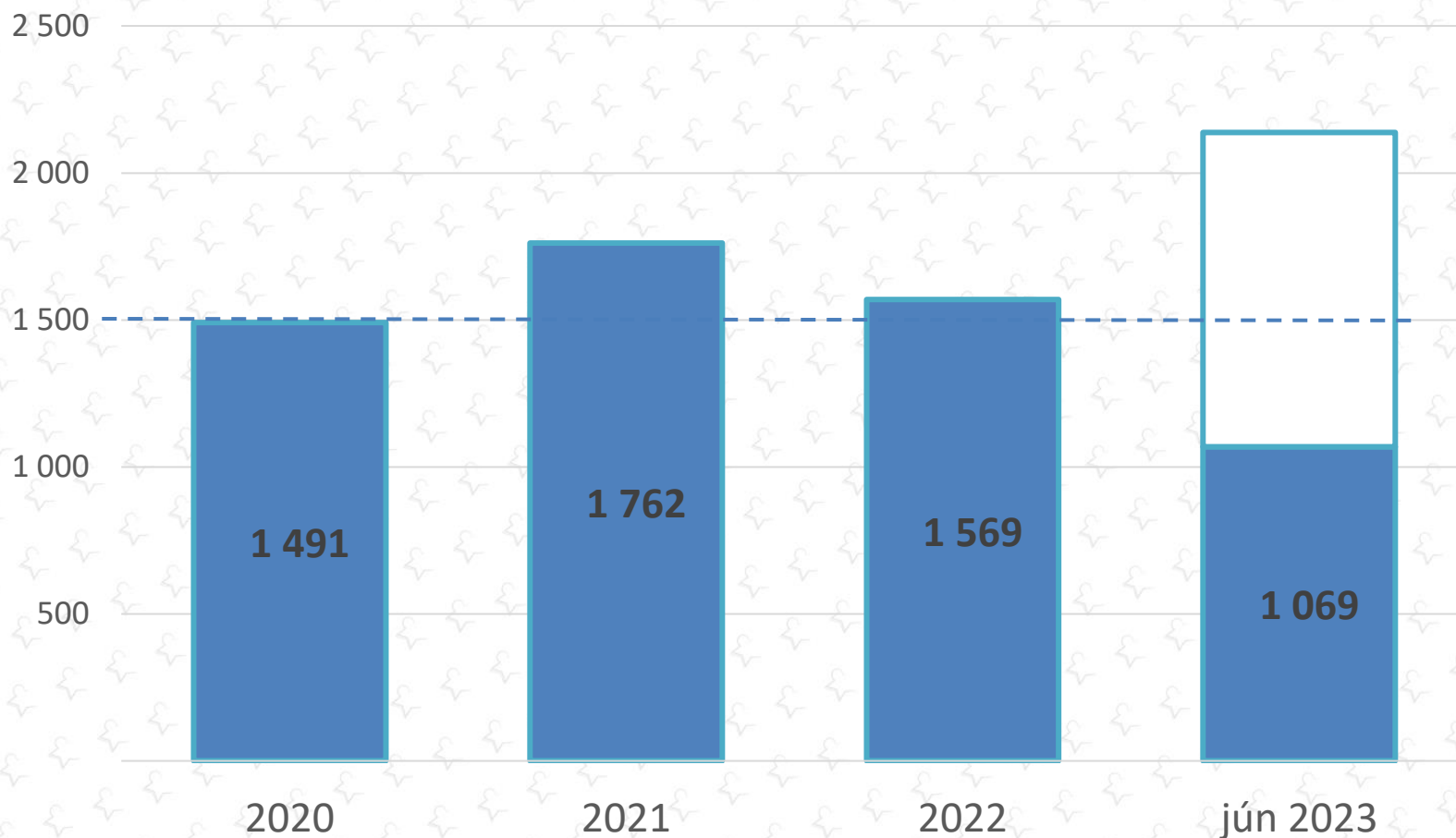
	Nápad	Obj.
§ 219 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty	<b>1585</b>	27 %
§ 247 Neoprávnený prístup do počítačového systému	37	2,7 %
§ 247a Neoprávnený zásah do počítačového systému	14	0 %
§ 247b Neoprávnený zásah do počítačového údajov -	19	9 %
§ 247c Neoprávnené zachytávanie počítačových údajov,	1	0 %
§ 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov	1	0 %



# § 219 Neoprávnené vyrobenie a používanie platobného prostriedku,



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE



Operačný program  
**Efektívna  
verejná správa**

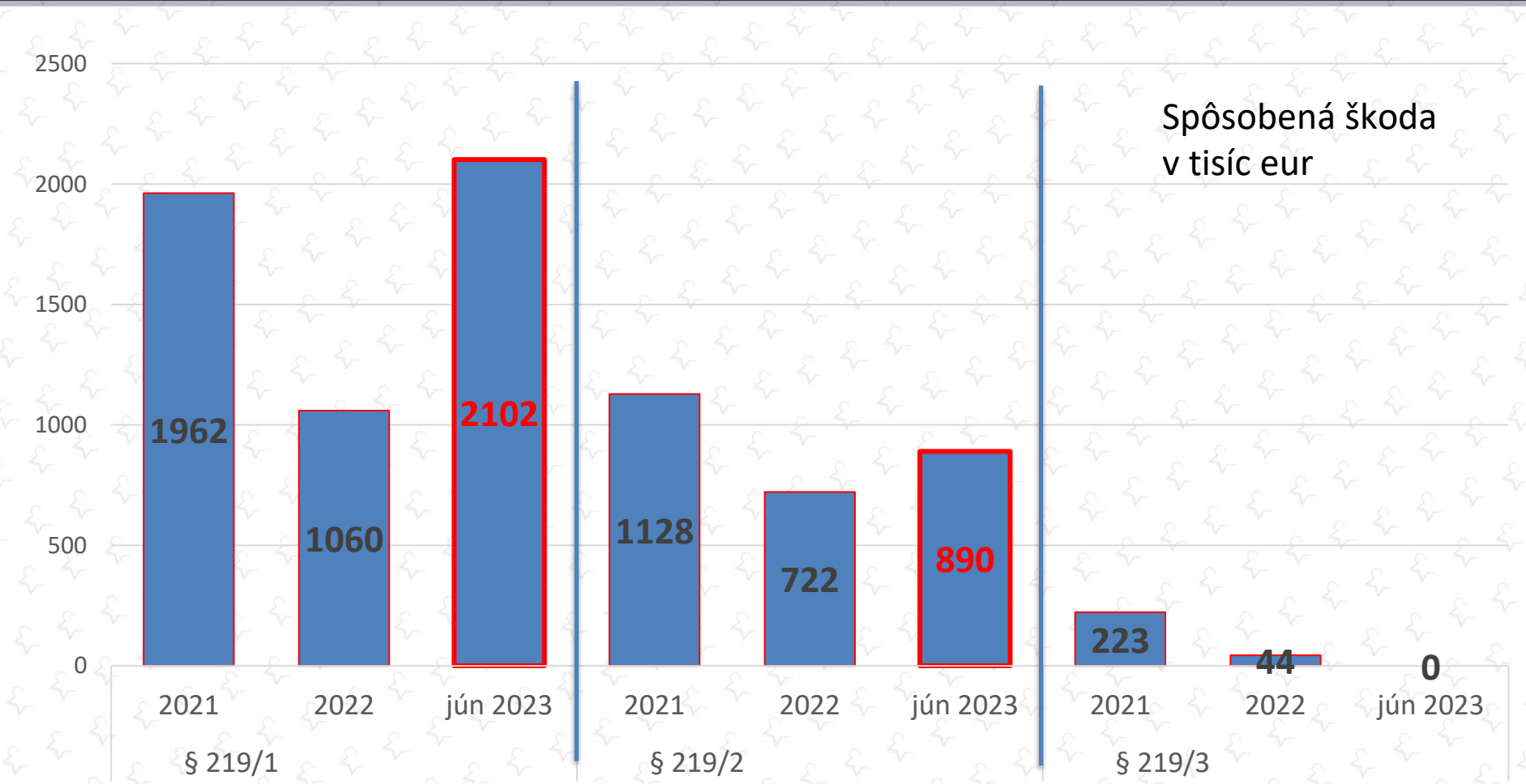


**Európska únia**  
Európsky sociálny fond



Zdroj údajov:  
OPK ÚKP P PZ

# § 219 Neoprávnené vyrobenie a používanie platobného prostriedku elektronických peňazí v SR



- ❑ v SR relatívne ↓ miera celkovej objasnenosti TČ (cca 30 %) spadajúcej pod PK je do značnej miery ovplyvnená
- európskou aj národnou legislatívou upravujúcou poskytovanie a uchovávanie dát elektronickej komunikácie (vrátane poskytovateľov internetového pripojenia), ktorá v súčasnosti nie je obligatórnou povinnosťou poskytovateľov elektronických služieb ani na minimálnu dobu (jedny z najdôležitejších dôkazných prostriedkov)
- nadnárodný rozmer
- rozmanitosť právnej úpravy,
- dynamika vývoja,
- zmeny v modus operandi.

Problémy a prekážky pri dokazovaní každej TČ vrátane pôsobenia HH.

# Boj proti legalizácii výnosov z TČ a financovaniu terorizmu

Medziročný **nárast** prepravy peňažných prostriedkov v hotovosti v 2022 oproti 2021 cez vonkajšie hranice SR Bol zaznamenaný o **606%**.

Zdroj: FSJ Výročná správa 2022.

## Hotovosť

- Pokles u spotrebiteľov
- Sofistikovanejšie využitie

## Bezhotovostný prevod

- Zanecháva digitálnu stopu
- ľahšie trasovateľné

	Počet oznámení	Prepravovaná suma
2021	83	2.812.308,74 EUR
2022	586	36.837.637,43 EUR



# Boj proti legalizácii výnosov z TČ a financovaniu terorizmu

Zákonné nástroje na systémovú elimináciu podvratnej činnosti pri legalizácii výnosov z TČ a financovaní terorizmu vrátane HH.

- Z č. 444/2015 Z. z. - novelizovaných 16 zákonov (tzv. protiteroristický balíček),
- Z č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov,
- Z č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov (tzv. protischránkový zákon, ktorý poskytuje väčšiu transparentnosť v oblasti obchodovania štátu so súkromným sektorom),

# Boj proti legalizácii výnosov z TČ a financovaniu terorizmu

- Z č. 52/2018 Z. z., ktorým sa novelizoval AML zákon,
- Z č. 346/2018 Z. z. o registri mimovládnych neziskových organizácii a o zmene a doplnení niektorých zákonov,
- v problematike konečných užívateľov výhod boli definovaní v AML zákone koneční užívatelia výhod právnických osôb a združení majetku,
- bol vytvorený Register partnerov verejného sektora.
- V apríli 2023 EP podporil nové EÚ pravidlá MiCA (*Markets in Crypto Assets*) umožňujúce sledovanie a identifikáciu prevodov kryptoaktív. Nový zákon umožňuje blokovanie podozrivých transakcií. Pravidlá sa vzťahujú na transakcie s kryptoaktívami nad 1 000 EUR.

- Ochrana finančného systému,
- Posilnenie mechanizmu na predchádzanie praniu špinavých peňazí a financovaniu terorizmu v rámci EÚ
- Výnimka zo starostlivosti vo vzťahu ku klientovi - podnikatelia poskytujúci služby s virtuálnymi menami nie sú povinní vykonať starostlivosť vo vzťahu ku klientovi napr. pri elektronických peniazoch uchovávaných na platobnom prostriedku, na ktorý nie je možné opakovane ukladať elektronické peniaze do 150 eur (v minulosti 250).

- Zneužívanie produktov v SR

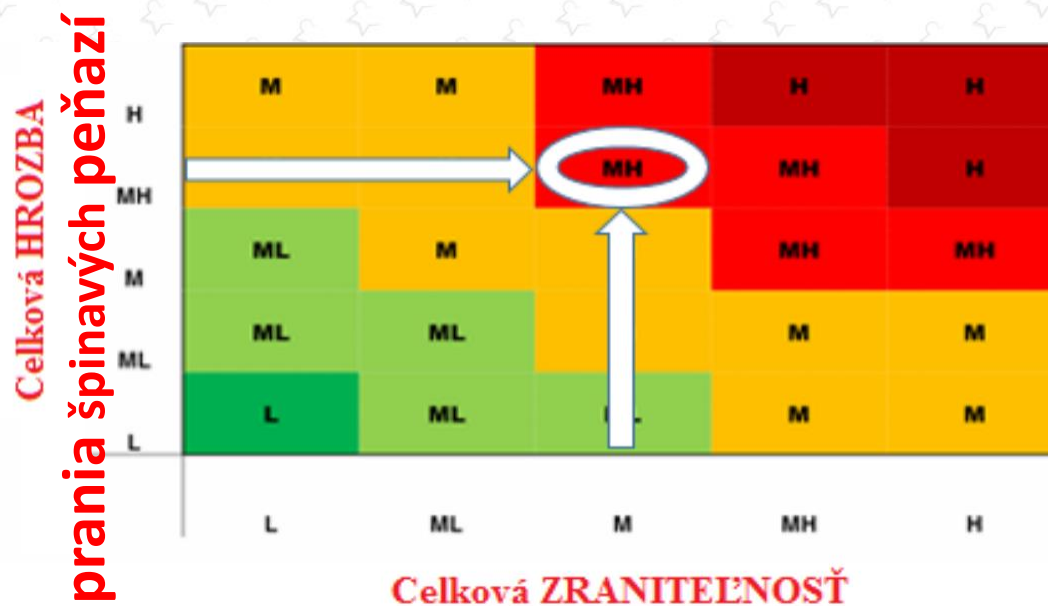
Ako možný súvis s ML/FT bolo zistené zneužívanie nastaveného systému v súvislosti so zasielaním šeku v akejkoľvek mene inej ako EUR, vyplatené prostredníctvom platobnej karty a následné vyplatenie šeku v hotovosti na pobočke Slovenskej pošty, a. s. Rádovo ide pri jednotlivých subjektoch o opakované transakcie, s viac ako stovkami uskutočnených návštev pobočiek Slovenskej pošty, a. s., v objemoch dosahujúcich státisícové hodnoty v EUR.



# Riziko legalizácie príjmov z TČ v SR



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE



Zdroj obrázka: Národné hodnotenie rizík legalizácie výnosov z TČ a financovanie terorizmu

Hrozby - skutočnosti alebo konanie osôb, ktoré môžu spôsobiť ujmu štátu, verejnosti či ekonomike.



Operačný program  
**Efektívna  
verejná správa**



**Európska únia**  
Európsky sociálny fond



# Riziko legalizácie príjmov z TČ v SR

	Predpokladaná výška nezaznamenaných výnosov z TČ	Hrozba ML					Trend
		5	4	3	2	1	
<b>Organizovaná TČ</b>	Podstatne vyšší	x					↓
<b>Počítačová kriminalita</b>	Podstatne vyšší		x				↑
<b>Environmentálna TČ</b>	(nepomerne) vyšší		x				↑
<b>Ekonomická TČ</b>	(nepomerne) vyšší		x				-
<b>Drogová TČ</b>	Podstatne vyšší		x				↑
<b>TČ korupcie</b>	Vyšší		x				-
<b>Majetková TČ</b>	Mierne vyšší				x		↓
<b>Násilná kriminalita</b>	<del>nedovolené ozbrojovanie a obchodovanie so zbraňami podstatne vyšší/nevýznamný</del>				x		↓
<b>Mravnostná TČ</b>	<del>Obchodovanie s ľuďmi vyšší/nevýznamný</del>				x		↑

# Virtuálna mena (kryptomena)

je digitálny nositeľ hodnoty, kt nie je vydaný ani garantovaný centrálnou bankou ani orgánom verejnej moci, nie je nevyhnutne naviazaný na zákonné platidlo, a ktorý nemá právny status meny ani peňazí, ale je akceptovaný niektorými FO alebo PO osobami ako nástroj výmeny, ktorý možno elektronicky prevádzať, uchovávať alebo s ním elektronicky obchodovať (TZ, AML zákon).

Použiteľný na:

- bežný nákup zákonom dovolených vecí
- Od 1.1.2024 ↓ daň z predaja kryptomien v SR  
(33 %-39 %+ zdravotné odvody 14 % jediný na svete)
- ☐ Krátkodobí investori < 1 rok 19 % alebo 25 % z dosiahnutého zisku
- ☐ Dlhodobí investori nad 1 rok 7 % z dosiahnutého zisku (v ČR 15 %)  
zdravotné odvody



# Virtuálna mena (kryptomena)

v prípade platby za tovary a služby kryptomenami oslobodenie od dane do 2 400 eur/rok. Nebude sa zdaňovať výmena jednej kryptomeny za inú.

Použiteľný na:

- bežný nákup zákonom dovolených vecí,
- uskutočňovanie nezákonných obchodov smerujúcich k predaju zbraní, drog, výroby, či rozširovaniu detskej pornografie a financovanie rozširovania HH.
- legalizácie príjmov z TČ.

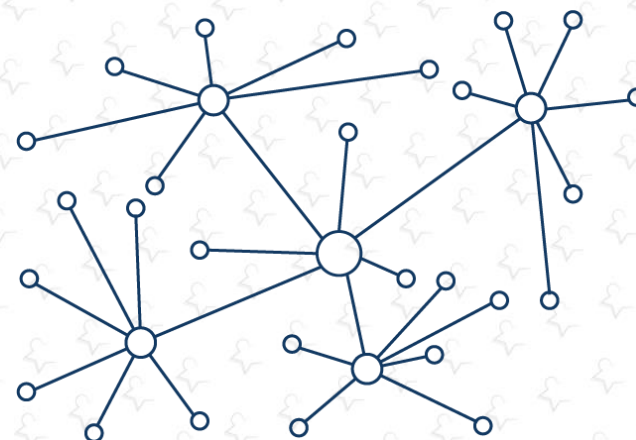




- je infraštruktúra,
- umožňuje rôznym distribuovaným softvérovým aplikáciám ukladať, uchovávať a sprístupňovať údaje,
- ukladá len základné údaje o transakciách, udalostiach
- distribuovaná- schopná uchovávať neustále sa rozširujúci počet záznamov, ktoré sú chránené proti neoprávnenému zásahu tak z vonkajšej strany, ako aj zo strany samotných uzlov siete,
- decentralizovaná,
- ,kombinácia kryptografických algoritmov a internetových sieťových protokolov



- Transparentnosť - každý účastník pozná aktuálny stav elektronickej účtovnej knihy
- Zapisovanie = konsenzus,
- neexistuje správca na určovanie chodu blockchainu
- bloky digitálnych záznamov na seba kryptograficky nadväzujú,



# Virtuálna mena (kryptomena)

text	MD5 Hash
hybridná	07b4ac354f91756bf35fda10f52227aa
hybridna	b3fc9b7c72bb2cc1820ed49ba4796406

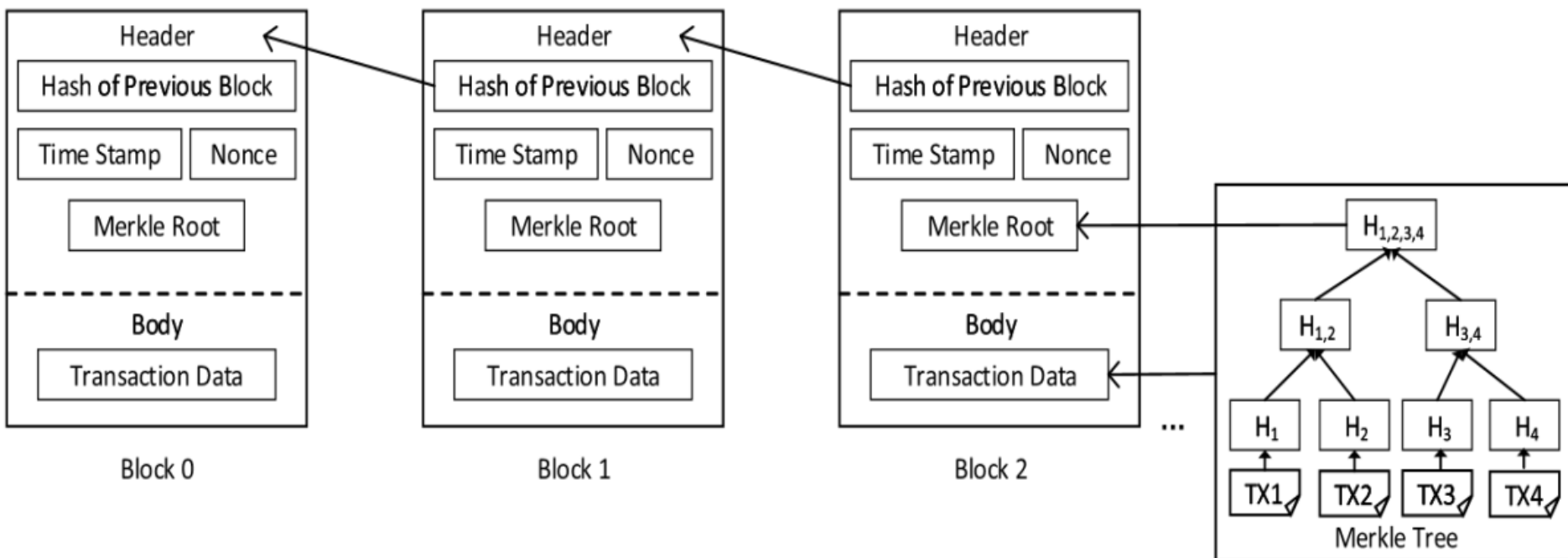
text	SHA1 Hash
hybridná	c2b38f6865f810f5cd45a4f077269d9e721baf0c
hybridna	66602b58233c5bd05d4308110bd71282e948f897



# Prednosti technológie blockchain



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE



Zdroj: Dostupné na internete: : <[https://link.springer.com/chapter/10.1007/978-981-15-0776-2\\_5/figures/1](https://link.springer.com/chapter/10.1007/978-981-15-0776-2_5/figures/1)>





- akákoľvek zmena v bloku predchádzajúcom ovplyvní všetky nasledujúce kryptografické výstupy blokov
- Po zápise dát nie je umožnená ich dodatočná zmena
- Automatická forma riešenia konfliktných transakcií - (snaha minúť sumu na účte viackrát) sa nikdy nestanú súčasťou potvrdeného datasetu.
- Zakázaním, vypnutím alebo napadnutím jedného alebo viacerých uzlov teda nedôjde k významnému narušeniu siete.
- s ↑ zodpovedných účastníkov siete virtuálnej meny ↑ aj celková bezpečnosť a stabilita vykonávania transakcií virtuálnej meny

- Najčastejšie spôsoby získania BTC peňaženky:
  1. Založenie účtu na kryptoburze
  2. Použitie online peňaženky
  3. Použitie offline peňaženky (odporúčané)

## Bitcoinová adresa/verejný kľúč



**VEREJNÁ  
INFORMÁCIA**

19PXg2Ljftt9hRj4R9xYjprsSw43ZhreSB

## Šifrovanie transakcií

Kryptograficky odvodený  
z privátneho kľúča

Služi na zdieľanie s tretími stranami

## Privátny kľúč



**TAJNÁ  
INFORMÁCIA**

KxJiXNGePRvbnfp1qFHGHCvtXF8662NnbVvkn6EgGtYt6Xzh9yPY

## dešifrovanie

Každý, kto má prístup k privátnemu  
kľúču, je disponantom kryptomeny

dôkaz o vlastníkovi kryptomeny/  
/disponentovi adresy

bezpečnostný mechanizmus na  
uskutočnenie kryptografických  
operácií vytvorenie samostatne

užívateľom/pomocou peňaženky VM

 **Sign/verify Message**

Message

I, the owner of address  
1Hta9NXidkpUeKTEzoVQuP1QoiqkZ4vj6M  
enjoy writing guides on privacy.

Address

1Hta9NXidkpUeKTEzoVQuP1QoiqkZ4vj6M|

Signature

H3FwKAAJjJ6nziW22fiWH9O7jgiXHACT+zSrd0  
Jlm9xGOYKEX/22QZr8vL0XmPW7w3nHjVOL  
B9K3GnXpMv9nBE=

Sign

Verify

Close

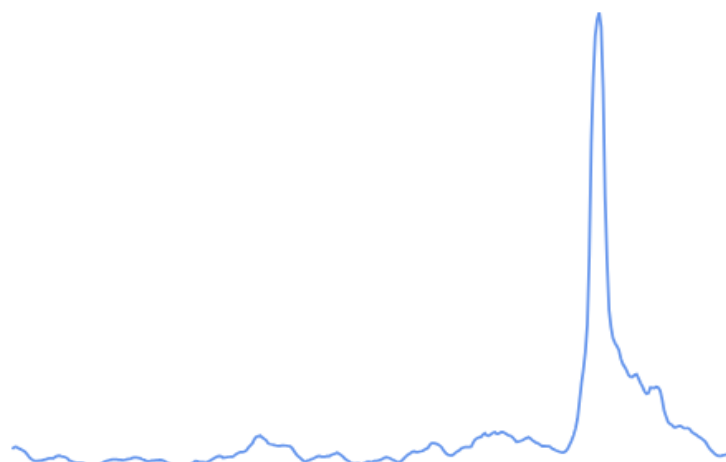
<https://www.expressvpn.com/blog/bitcoin-anonymity/#how-you-can-be-deanonymized-using-bitcoin>



# Technológia blockchain – typy záznamov

- **Transakcie** - dáta vložené do databázy užívateľa

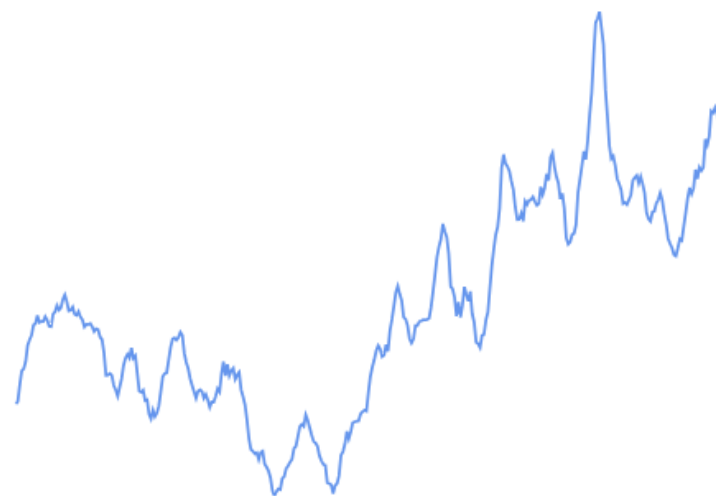
Total Transaction Fees (BTC)



The total BTC value of all transaction fees paid to miners. This does not include coinbase block rewards.

- **Bloky**- na validovanie transakcií a záznamy, kedy a ako bola konkrétna transakcia

Miners Revenue (USD)



## Bitcoinové transakcie

Sú všetky verejné a možno ich sledovať prostredníctvom blockchainového explorera.



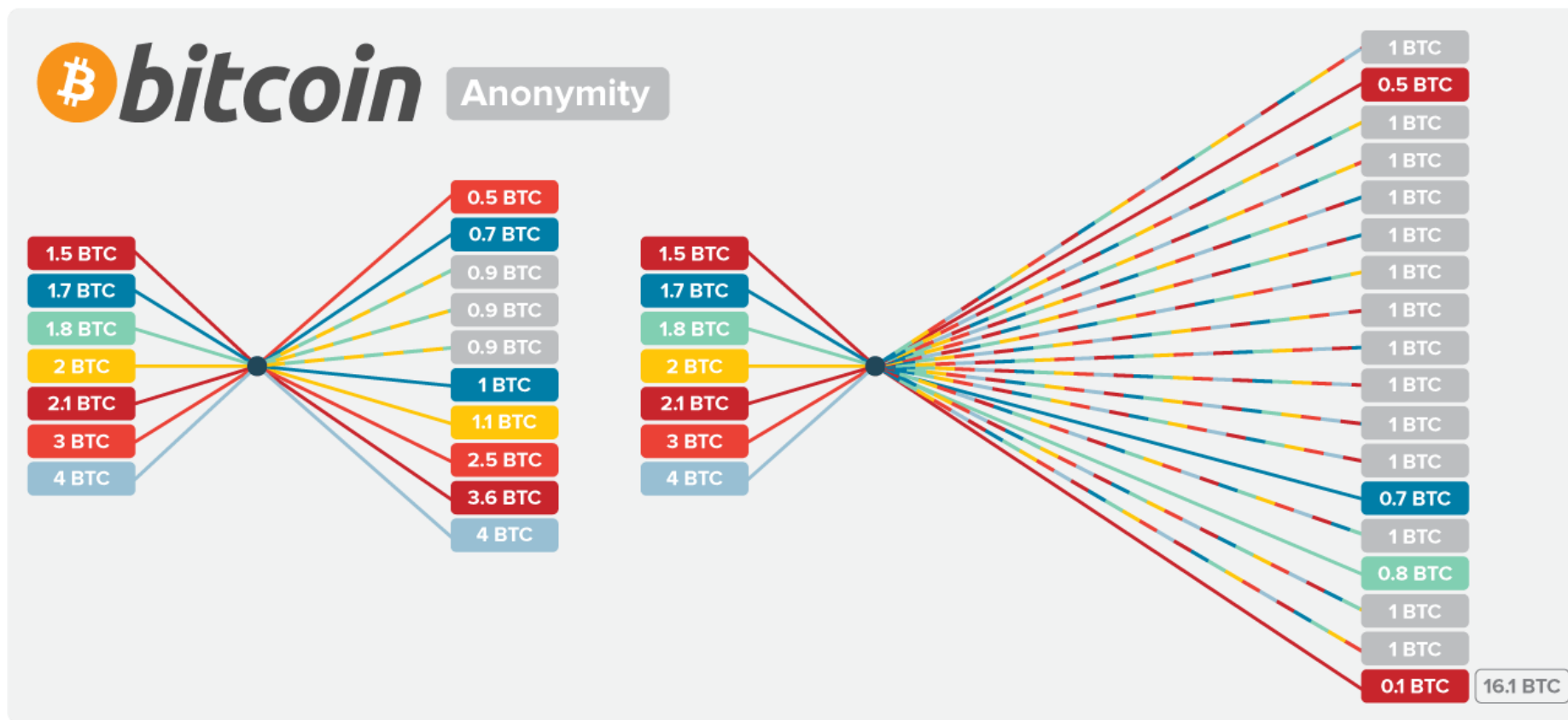
### Latest Transactions Bitcoin



dd56c-35307	14:57:00	0.00125602 BTC	\$37.40
15168-dc09f	14:57:00	0.00125602 BTC	\$37.40
a0788-e3aa6	14:57:00	0.01193133 BTC	\$355.28
948b5-f605f	14:57:00	0.02715241 BTC	\$808.52
83710-48566	14:57:00	0.00125602 BTC	\$37.40
45464-2892d	14:57:00	0.00125602 BTC	\$37.40



# Mixovanie transakcií



Zdroj: <https://s22908.pcdn.co/wp-content/uploads/2017/10/image1.png>

# Virtuálne meny – mixovanie transakcií



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE

Bitcoin Mixer	Main Features	Mixing Time
<a href="#">Unijoin</a>	<ul style="list-style-type: none"><li>• Pay as You Wish</li><li>• Minimum of 0.01 BTC.</li></ul>	3 blockchain confirmations
<a href="#">Sinbad.io</a>	<ul style="list-style-type: none"><li>• No registration</li><li>• Minimum of 0.001 BTC</li></ul>	3 blockchain confirmations + up to 10 min
<a href="#">Mixero</a>	<ul style="list-style-type: none"><li>• No registration</li><li>• Minimum of 0.002 BTC</li></ul>	1 blockchain confirmation – 2 hours
<a href="#">Yo!Mix</a>	<ul style="list-style-type: none"><li>• No registration</li><li>• Uses predefined a wallet</li></ul>	1 blockchain confirmation
<a href="#">Coinomize</a>	<ul style="list-style-type: none"><li>• User-controlled time delays</li><li>• Allows extra payout addresses</li></ul>	1 blockchain confirmation

Supported Systems: Web Browser/ Tor

Zdroj: <https://coinmarketcap.com/community/articles/64340c9b854d003676188835/>







Pozitíva mixovania	Negatíva mixovania
↑ súkromie transakcií	Centrálny mixér ↑ riziko úniku dát
Poskytuje anonymitu	Ak neoverený mixér ↑ riziko mix so špinavými peniazmi
↑ ochrana pred krádežou	Mixovanie ako služba za poplatok



# Volatilita virtuálnej meny



AKADÉMIA  
POLICAJNÉHO ZBORU  
V BRATISLAVE

\$30,086.13 • 06:00

Vol 19 BTC

1D 1W 1M 1Y MAX USD

Deň 15.7.2023



\$30,040.39 • 23:30

Vol 23 BTC

1D 1W 1M 1Y MAX USD

Týždeň 11.-17.7.2023



\$30,322.80 • Jul 16 13

Vol 126 BTC

1D 1W 1M 1Y MAX USD

Mesiac 18.6.-16.7.2023



\$30,285.58 • Jul 10

Vol 4,817 BTC

1D 1W 1M 1Y MAX USD

Jrok úl 2022-jún 2023

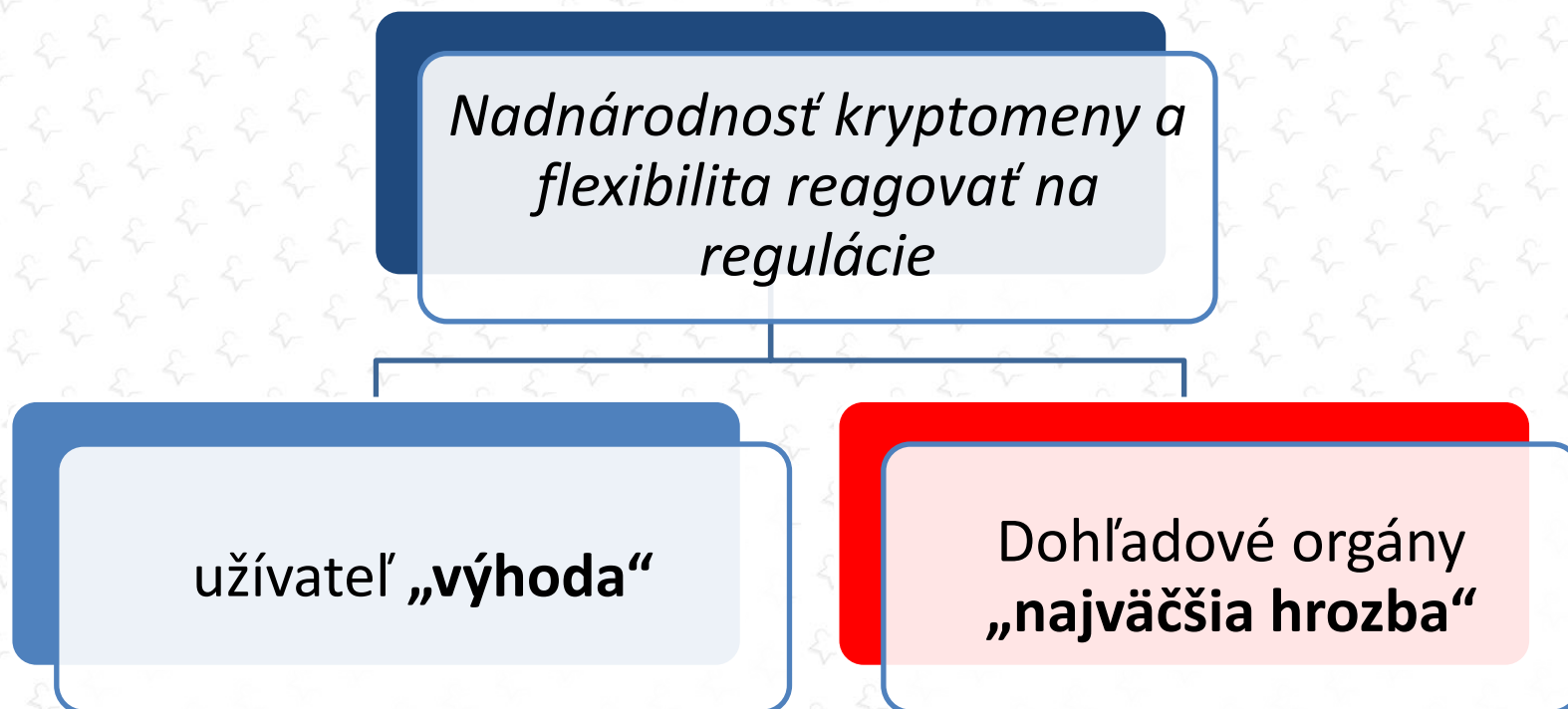


Operačný program  
**Efektívna  
verejná správa**



**Európska únia**  
Európsky sociálny fond





Obchádzanie sankcií a transfer ruského kapitálu do zahraničia cez kryptoaktíva. Hrozby spojené nielen s AML ale i geopoliticko-bezpečnostné hrozby.

## Trestný poriadok § 96d

### Zaistenie virtuálnej meny

Ak zistené skutočnosti nasvedčujú tomu, že VM je nástrojom TČ alebo výnosom z TČ, môže predseda senátu a v prípravnom konaní prokurátor vydať príkaz na zaistenie VM, pri ktorom sa zakážu akékoľvek dispozície s VM a prikáže sa jej vydanie vrátane vydania hesla, prístupového kódu alebo podobných údajov umožňujúcich nakladanie s VM. Právne úkony urobené v rozpore so zákazom podľa predchádzajúcej vety sú neplatné. Eviduje sa:

- Typ kryptomeny,
- Typ peňaženiek,
- prevádzkovateľa kryptoburzy v prípade ak boli využívané,
- či sú peňaženky na úschovu kryptomien chránené heslom.



- Pseudoanonymné – bez personálnych dát,
- Nevedie sa evidencia, kto je držiteľom alebo vlastníkom privátneho kľúča (ochrana je v kompetencii účastníka siete).
- Prevod virtuálnej meny je cez internet veľmi rýchly.
- Cez zálohovanú bitcoinovú peňaženku (vyšetrovateľ o nej nemusí vedieť) môže spraviť prevod akákoľvek osoba z akéhokoľvek zariadenia s prístupom na internet a kedykoľvek.
- Pri prevode virtuálnej meny už nie je možný prevod späť.

# Zaistovanie virtuálnej meny v trestnom konaní OČTK

- znalecké skúmanie elektronických zariadení, prípadne mobilných telefónov, v ktorých sa hľadá zálohový súbor elektronickej peňaženky. Bez súčinnosti osoby, ktorá pozná heslá k adrese s najväčšou pravdepodobnosťou k faktickému zaisteniu kryptomeny ako nositeľovi hodnoty nedôjde.
- Pri skúmaní zaistenej výpočtovej techniky sa hľadá zálohový súbor elektronickej peňaženky. Ak sa podarí získať aj heslo do peňaženky, obnovením zálohového súboru je možné získať prístup k privátnym kľúčom peňaženky.
- Hrozba je spojená so zlou trasovateľnosťou financovania napr. podvratnej činnosti.

# Zaistovanie virtuálnej meny v trestnom konaní OČTK

## Centralizované burzy

- Sprísňujú starostlivosť o klientov (podrobnejšie preverujú osoby, pôvod financií, prísnejšie dozerajú na tok transakcií.
- môže obmedziť prístup k svojej kryptomene, obmedziť alebo zastaviť obchodovanie s ňou

## Decentralizované burzy DEX

- Výmena VA na rôznych sieťach
- Funguje len s kryptomenami (fiat)
- Každý je zodpovední za svoju bezpečnosť.
- Nárast počtu v Ruskej federácii

# ČLR predstavuje rastúcu komplexnú spravodajskú hrozbu.

- **Z. o štátnej bezpečnosti (2015)** ukladá všetkým čínskym občanom a organizáciám všeobecnú povinnosť poskytnúť pomoc štátnym orgánom v otázkach štátnej bezpečnosti.
- **Z. o štátnej spravodajskej činnosti (2017) čl. 7** - každý občan a organizácia musí podporiť národnú spravodajskú činnosť, poskytnúť súčinnosť a spoluprácu a zachovať mlčanlivosť o utajovaných záležitostiach, o ktorých sa v súvislosti s národnou spravodajskou činnosťou dozvie.
- **Zákon o obchodných spoločnostiach (2013)** umožňuje KSČ účinne ovplyvňovať chod súkromných spoločností. Podľa čl. 19 musí byť v spoločnosti ustanovená organizácia KSČ za účelom výkonu aktivít KSČ v zhode s jej stanovami, pritom spoločnosť musí pre tieto aktivity poskytnúť nevyhnutné podmienky.

Zdroj: Národný  
úrad pro  
kybernetickú a  
informačnú  
bezpečnosť



# ČLR predstavuje rastúcu komplexnú spravodajskú hrozbu.

- **Z. o štátnej kontrašpionážnej činnosti (2014)** ukladá povinnosť poskytnúť súčinnosť a info. o zahraničných klientoch čínskych spoločností ak ich budú štátne orgány podozrievať zo špionážnej činnosti. Podľa čl. 6 je tento Z. aplikovateľný i voči inštitúciám, organizáciám a jednotlivcom, kt. organizujú alebo financujú špionážnu aktivitu proti ČLR mimo jej teritórium (za špionáž môžu čínske orgány označiť široké množstvo aktivít bez možnosti nezávislého súdneho skúmania).
- Po schválení a zavedení kryptografického Z je v Číne zakázané šifrovanie dát a v prípade šifrovania sú podnikatelia nútení poskytnúť šifrovacie kľúče. KSČ má prístup ku všetkým dátam zahraničných firiem podnikajúcich na území Číny.

Zdroj: Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

# ČLR predstavuje rastúcu komplexnú spravodajskú hrozbu.

- Podľa **pravidiel pre nahlasovanie zraniteľností v sieťových zariadeniach** v ČLR z roku 2021 majú výrobcovia technológií povinnosť nahlasovať bezpečnostné zraniteľnosti M priemyslu a IT(MPIT) najneskôr do 2 dni od zistenia. MPIT nahlasuje nález M štátnej bezpečnosti ČLR a ďalším relevantným inštitúciám.
- Je zakázané zverejňovať tieto zraniteľnosti alebo ich nahlasovať zahraničným organizáciám a jednotlivcom.

Zdroj: Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

- Vyvinutá a prevádzkovaná čínskou spoločnosťou ByteDance
- Celosvetovo najpopulárnejšia vo svojej kategórii (v Čechách 2 mil.)
- Primárne zdieľanie videí s trvaním do 15 sekúnd alebo dlhších príbehových videí do 60 sekúnd pre mobilné zariadenia.
- Modifikovanie videí prostredníctvom rôznych grafických alebo hudobných efektov a filtrov.
- Nepísaným pravidlom bezpečnosti je, že čím viac osôb je zúčastnených na istej činnosti, tým hrozí väčšia koncentrácia páchatel'ov TČ.
- Z hľadiska bezpečnosti v kyberpriestore platí podobne, čím viac majú aplikácie a sociálne siete používateľov, tým sú atraktívnejšie pre kybernetických útočníkov.

- popularita tejto formy rýchlo a jednoducho pochopiteľného obsahu podporila vznik mnohých extrémnych a často nebezpečných výziev (často nebezpečné aktivity, ktoré užívatelia následne zdieľajú na platforme)
- Šírenie CSAM materiálov,
- Zbiera obrovské množstvo užívateľských dát
- = > možnosť vydierania, nátlaku,
- Vynucovania



Zdroj obrázka: <https://www.istockphoto.com/>



- Mapovanie zariadení, kedy aplikácie zisťujú info o iných spustených a inštalovaných aplikáciách,
- obsah súkromnej komunikácie je ukladaný na servre ByteDance,
- pravidelná kontrola lokalizácie zariadení,
- info o zariadeniach vrátane Wi-Fi SSID, predchádzajúcej konfigurácii Wi-Fi, sériového čísla zariadenia a SIM karty, ID zariadení, IMEI zariadení, MAC adresy, telefónneho čísla, zoznam všetkých užívateľských účtov používaných na zariadeniach a kompletného prístupu ku schránke.
- Perzistentný prístup ku kalendáru umožňujúci jeho čítanie a zmenu,
- Vynucovanie využívania natívneho prehliadača, ktorý umožňuje sledovať takmer každú aktivitu užívateľa.

- Množstvo ľahko zneužiteľných dát/spôsob zbierania môže slúžiť ku vydieraniu konkrétnych záujmových osôb (politické špičky, verejní činitelia či strategicky dôležité osoby organizácie).
- Mobilné zariadenia sú v mnohých prípadoch súčasťou IS regulovaných Z. o KB/kritickej informačnej štruktúry/IS základných služieb a pristupujú tak ku kľúčovým aktívam tvoriacim regulované systémy. Narušenie bezpečnosti takýchto mob. zariadení vedie k priamemu ohrozeniu bezpečnosti regulovaných systémov – ohrozené riadne poskytovanie služby, pre kt. boli tieto systémy do regulácie zaradené.
- ByteDance verejne deklaruje - dáta užívateľov z Európy sú uložené na území USA a Singapuru, ale vzdialený prístup udelený niektorým subjektom v Brazílii, ČLR, Malajzii, Singapuru, USA a na Filipínach.

- EK vyšetruje, či vzhľadom na rozsiahly zber dát, ktoré aplikácia TikTok uskutočňuje, nie je nakladanie s nimi a prístup k nim v rozpore s Nariadením Európskeho parlamentu a Rady (EU) 2016/679 zo dňa 27. apríla 2016 o ochrane FO v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov a o zrušení smernice 95/46/ES (všeobecné nariadenie o ochrane OÚ).
- USA, Kanada, Dánsko, ČR, Lotyšsko, UK - zákaz používania TikToku vo všetkých vládou vydaných mobilných zariadeniach. Flámska regionálna vláda rozhodla zablokovat' prístup k čínskej videoaplikácii TikTok na telefónoch a počítačoch svojich zamestnancov. K takémuto opatreniu pristúpila po odporúčaní viacerých bezpečnostných a kybernetických agentúr.
- India, Irán úplný zákaz

- Závažná kybernetická hrozbu spojenú s inštaláciou a používaním aplikácie TikTok
- predstavuje vysoké riziko narušenia integrity bezpečnosti (úroveň Vysoká – Hrozba je pravdepodobná až veľmi pravdepodobná).
- eliminovanie predmetnej hrozby, **aplikáciu TikTok odinštalovať a zakázať jej inštaláciu na všetkých zariadeniach** (služobné/pracovné zariadenia aj súkromné zariadenia využívané na pracovné účely), ktoré majú prístup do IS a infraštruktúry MV SR.



- Kyberzločinci začali aktívne zneužívať chatbotov na to, aby zaujali a odpútali pozornosť potenciálnych obetí.
- nedostatok regulácie – V tomto prostredí chýba regulačný dohľad. Zvyšuje to riziko spojené s kyberzločinom.
- Schopnosť tvoriť automatizovane text podľa požiadaviek objednávateľa je nebezpečná hrozba z hľadiska ťažko kontrolovateľného vplyvu na verejnú mienku formou blogov, diskusných príspevkov na sociálnych sieťach, na internete ako aj generovanie spamov a ich následné rozposielanie, tvorba phishingových e-mailov.



# Hrozby sociálnych sietí pre základné práva a demokraciu

- Neposielať a nevkladať žiadne osobné údaje, interné, citlivé a dôverné informácie. Vložené údaje môžu byť uchovávané a použité bez vedomia dotknutej osoby a nielen na marketing (externí používatelia).
- zlučovanie poskytnutých info do nových info => neočakávané/negatívne výsledky.
- rozdeľovanie a polarizácia vo verejnej sfére a manipulácie s voľbami.
- Stopovanie a profilovanie jednotlivcov podľa ich názorov alebo konania.

PATRO, Tomáš. Umelá inteligencia: Čo to je, ako funguje a prečo je dobré sa o ňu zaujímať?. *Bud' FIT* [online]. 2017

POTH, Rachelle Dene. Artificial Intelligence: Implications for the Future of Education. *Getting Smart* [online]. 2018

POTH, Rachelle Dene. Artificial Intelligence: Implications for the Future of Education. *Getting Smart* [online]. 2018 Dostupné z: <http://www.gettingsmart.com/2018/01/artificial-intelligence-implications-for-the-future-of-education/>

PURPLESEC. 2019 Cyber Security Statistics Trends & Data. [online]. Dostupné na internete: <https://purplesec.us/resources/cyber-security-statistics>

MIRKOVIC, J. – REIHER, P. 2014. A taxonomy of DDoS attack and DDoS defense mechanisms. In ACM SIGCOMM Computer Communications Review, 2014, roč. 34, č. 2, s. 39

ZARGAR, S. T. – JOSHI, J. – TIPPER, D. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. In Communications Surveys & Tutorials, 2013, roč. 15, č. 4, s. 2049

ZEMKOVÁ, E., & HAMAR. D. 2009. Towards an Understanding of Agility Performance, Albert, 2009. - ISBN 978-807326-168-9

MIŠOTA, M. Ransomvérové skupiny, ransomvérové útoky a exfiltrácia údajov In: Bezpečnosť elektronickej komunikácie [elektronický dokument] : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. - Bratislava : Akadémia Policajného zboru v Bratislave, 2022.

[online]. [https://www.bezpek.eu/wp-content/uploads/2023/03/Bezpecnost-elektronickej-komunikacie\\_2022.pdf](https://www.bezpek.eu/wp-content/uploads/2023/03/Bezpecnost-elektronickej-komunikacie_2022.pdf)- ISBN 978-80-8054-968-8.

WESTERLUND, M., 2019. The Emergence of Deepfake Technology: A Review. [online] [cit. 14.05.2022]. Dostupné na internete:

[https://www.researchgate.net/publication/337644519\\_The\\_Emergence\\_of\\_Deepfake\\_Technology\\_A\\_Review](https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review)

INCAPSULA, Inc. 2017. Denial of Service Attacks.

GLOBSEC. 2019. Hybridné hrozby na Slovensku

CoEC. 2001. Commission of the European Communities. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach.

Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov



# Otázky?



Zdroj obrázka: <https://www.istockphoto.com/>

# Ďakujem za pozornosť