BPC-KKR

Kyberkriminalita

Otázky ke státnicím

Bakalářský obor Informační bezpečnost, FEKT VUT

https://github.com/VUT-FEKT-IBE/BPC-IBE-SZZ

Text: Yakub, Vikča
Korektura: –

25. května 2022

Obsah

1 Vzájemný vztah pojmů kyberkriminalita, kybernetická bezpečnost a kybernetická obrana.

Liší se v tom KDO CO provádí za JAKÝM účelem a za pomoci JAKÝCH prostředků.

1.1 Kyberkriminalita

Obecný pojem, který lze chápat v užším nebo širším smyslu - v užším smyslu do něj zahrnujeme **trestnou činnost**, která směřuje právě přímo proti důvěrnosti, dostupnosti, či integritě informačních systémů (neoprávněný přístup k počítačovému systému a nosiči informací, nebo opatření a přechovávání hesla a přístupového zařízení k počítačovému systému).

V širším smyslu lze zahrnout další dvě kategorie trestné činnosti - **tradiční trestnou činnost**, která je páchána prostřednictvím informačních a komunikačních technologií - tedy například podvod, nebo výroba a jiné nakládání s dětskou pornografií, a **trestná činnost** při jejímž páchání je využito informačních a komunikačních technologií incidentálně, přičemž se při jejím vyšetřování dají čerpat elektronické důkazní prostředky.

Kyberkriminalitou se zabývají orgány činné v trestním řízení - tedy především policie, státní zastupitelství a soudy. Primárními nástroji využívány orgány činnými v trestním řízení jsou procesní postupy definované trestním řádem - tedy především zajišťování elektronických důkazů pomocí odposlechů, zajišťování dat, forenzní analýzou, apod.

1.2 Kybernetická bezpečnost

je aktivita, která spočívá v monitoringu počítačových infrastruktur, jejímž cílem je zjistit výskyt zranitelností těchto infrastruktur, případně kybernetických bezpečnostních incidentů. Kybernetická bezpečnost tedy mimo technických nástrojů zahrnuje rovněž nástroje právní a organizační. Jejím cílem je primárně zajistit CIA triádů (dostupnosť, integritu a dôvernosť informácií) spravovaných infrastruktur. Kybernetickou bezpečnost zajišťují na úrovni organizací takzvané CSIRT týmy, které sledují a zabezpečují svoji izolovanou infrastrukturu, na úrovni státu je to v případě ČR Národní a Vládní CERT tým, které koordinují postupy provozovatelů sítí a systémů. Na mezinárodní úrovni jsou to různé mezinárodní organizace a dobrovolné spolky, které především umožňují sdílení informací (například ENISA).

1.3 Kybernetická obrana

je obrana proti kybernetickým útokům, které mají charakter vojenského útoku, které objektivně ohrožují suverenitu státu. Kybernetická obrana státu by tak měla spočívat v budování schopností vojenských složek ubránit národní infrastrukturu proti takovým útokům a budovat za tím účelem dostatečně akceschopné jednotky. V ČR má na starosti kybernetickou obranu resort Ministerstva obrany a především Vojenské zpravodajství (jde o vojenskou rozvědku a kontrarozvědku).

2 Prameny práva (národní, evropské i mezinárodní) obsahují hmotněprávní a procesněprávní úpravy kyberkriminality.

2.1 Hmotněprávní úpravy

Třestní zákoník č. 40/2009 Sb. ve znění pozdějších předpisů – popis trestního práva hmotného - obsahuje

- obecnou část (obecná definice pojmů, co je trestný čin, jaké jsou možnosti trestu, urhný x souhrný trest, polechčující okolností, promlčení, kdo může být pachatelem, zavinění (umysl x nedbalost))
- zvláštní část, kde je popis jednotlivých skutkových podstat trestných činnů - jsou definovány skutkové podstaty týkající se přimo kyberkriminality - neopravněný přístup k poč. systému §230, příprava hack nástroju §231 - nebo jsou součástí skutkových podstat týkajících se běžné trestné činosti - porušení tajemstí §182, porušení autorského práva §270, dětská pornografie §192, nebezpečné pronásledování §354, podvod §209 - v těchto případech se často jedná o kvalifikovanou skutkovou podstatu nebot ICT umožňují snažší páchání daného TČ s větším dopadem.

2.2 Procesněprávní úpravy

Trestní řád - popisuje trestní právo procesní - definuje samotný proces a jeho fáze, zúčastněné osoby, obviněný, poškozený, obhájce a jejích postavení v třestním řízení - definuje zásady/postupy trestního řízení/stíhání (procesní nástroje) - obecná součinnost §8, freezing §7b, odposlech §88, zajištění provozních a lokalizačních údajů §88a odst. 1, sledování osob a věcí §158d - některé nástroje jsou přímo spjaty s ICT (freezing, metadat), jiné jsou nejsou původně zamýšleny pro ICT ale jsou tak nyní používané (sledování osob a věcí, pro získání dat od ISP).

Další prameny práva upravy kyberkriminality:

- Zákon o elektronických komunikacích č. 127/2005 Sb
  - Data retention – uchování provozních a lokalizačních údajů po dobu 6 mesíců
- Úmluva o kyberkriminalitě
- Směrnice o útocích na informační systémy
- Evropská úmluva o vzájemné pomoci ve věcech trestních č. 550/1992 Sb. (mezinárodní trestní právo)
- Zákon o mezinárodní justiční spolupráci ve věcech trestních č. 104/2013 Sb. (mezinárodní trestní právo)

  - definuje justiční spolupráci MLA - **Evropský vyšetřovací příkaz** (založen na uznávání příkazů - MR)
- CLOUD act

3 Úmluva o kyberkriminalitě a směrnice o útocích na informační systémy (obsah úpravy a vztah k české právní úpravě)

Úmluva o kyberkriminalitě je nejúspěšnější instrument práva mezinárodního veřejného v oblasti kyberkriminality - vydána roku 2001 - ČR podepsala roku 2005 - ratifikace roku 2013 - ratifikováno 65 státy - další státy provedli třeba teprve část a zbytek je pro ně problematický implementovat nebo jim to trvá déle - vpodstatě i u nás - až roku 2013 jsme dokončili implementaci, přijetím zákona o trestní odpovědnosti právnických osob - velmi podobná je se **Smernicí o útocích na informační systémy** - směrnice EU ale skutkové podstaty jsou formulované v podstatě stejně - tyto dva úpravy jsou hlavní zdroje mezinárodního práva, které ovlivňují právní úpravu v ČR - jsou v jich definované skupiny trestných činů - Zločiny proti důvěrnosti, interitě a dosažitelnosti systému - Zločiny se vztahem k počítači a k přenášenému obsahu (zásahy do soukromí) - Zločiny se vztahem k autorským právům

K Úmluvě o kyberkriminalitě byl podepsán první dodatkový protokol (kriminalizace činů rasistické a xenofobní povahy spáchané prostřednictvím počítačového sytému) - který se týka dětské pornografie - v Radě Evropy pracuje skupina odborníků na druhém dodatovkém protokolu - který by měl řešit problém s omezenou možností spolupráce (nové procesní nástroje pro exektivní předávání dat, videokonference, mechanismus předávání dat apod)

Vznikla kvůli problémům mezinárodního práva - snaží se tedy harmonizovat - podepsalo 44 států - z nečlenských států pouze USA - udává, aby sankce byly účinné, přiměřené a odstrašující

Problém úmluvy je že je z roku 2001 a nereflektuje tedy aktuální stav - a další problém je že nepokrývá vše, neboť nedošlo ke společnému konsenzu

Nastavuje procesní věci, které zjednodušují mezinárodní justiční spolupráci - sjednocuje procesní nástroje - pro spolupráci je potřeba dvojítrestnost + musí mít nástroje pro vyhovění

Úmluva o kyberkriminalitě říká, že v právním řádu jednotlivých států (procesní nástroje úmluvy) musí být zajištěné:

- urychlené uchování dat (freezing) - TŘ §7b
- urychlené uchování a vydání provozních a lokalizačních údajů - má existovat vydávací příkaz - možnost prohledání a zajištění dat - v Zákoně o elektornických komikacích

- vydání věci - trestní zákoník
- možnost odposlechu komunikace - TŘ §88
- musí existovat orgán, který dokáže ve dne v noci 24/7 tuto spolupráci realizovat
- mechanizmus pro dobrovolné předávání informací - dále je v umluvě upraven způsob využití těchto procesních nástrojů - stále je to všechno postaveno na MLA - mezinárodní justiční spolupráci - úprava v trestním řádu
- možnost přímého přístupu k datům v zahraničí při souhlasu

4 Postupy a kriteria při kvalifikaci trestné činnosti (vč. problematiky kvalifikované a privilegované skutkové podstaty)

Postupy a kriteria při kvalifikaci trestné činnosti:

- zjištění zda jde o TČ nebo ne - OČTŘ - formální pojetí TČ - zjištění jestli skutkové okolnosti naplňují formální znaky skutkové TČ pospsaného v TZ ve zvláštní části – **právní kvalifikace**
- okolnosti vyloučení protiprávnosti - některé TČ jsou trestné pouze za určitých okolností (místo, čas, způsob) - promlčení
- odpovědnost podezřelého - věk, příčetnost
- určení zavinění - úmysl a nedbalost
- zohlednění účinnosti Trestního práva - zásady jusrisdikce - teriotrialita, registrace, personalita, ochranná a univerzální
- zjištění zda jeden spáchaný skutek nenaplňuje znaky i dalších trestných činnů, subsumpce pod více TČ
- souběh TČ a jejich vyloučení - pachatel nesmí být potrestnán dvakrát za jeden čin
- určení míry trestu - kvalifikovaná skutková podstata, polechčující přitěžující okolnosti, úhrný a souhrný trest

4.1 Právní kvalifikace

Právní posouzení určitého jednání – jde o rozhodnutí zda spáchaný skutek/čin byl nebo nebyl TČ pokud - byl tak daný skutek zařazen pod odpovídající TČ.

Dále se posuzují trestněprávní odpovědnosti obviněného a okolnosti případného obvinění, nepříčetnosti obviněného, polehčující a přitěžující okolnosti a podobně - dále se určuje např zavinění (úmysl x nedbalost) - dále se řeší souběh (a vyloučení souběhu, úhrný a souhrnný trest, zajištění aby pachatel nebyl potrestán dvakrát za stejný čin).

Kvalifikace začíná podmětem k TČ a končí soudním rozsudkem, který ukončí/provede konečnou kvalifikaci a udělí trest v případě odsouzení, může taky neodsoudit (shledat obžalovaného nevinným) - kvalifikace se v průběhu trestního stíhání může měnit - jednotlivá vyjádření jsou ve fázích zahájení (OČTŘ) TS - obžaloba (státní zástup) - rozsudek (soud) a další - kvalifikace se tak může měnit (očtř, státní zástupce a soud na sebe nejsou závislé, každý dělá svojí kvalifikaci)

4.2 Skutek

Činnost obviněného, která má za následek porušení nebo ohrožení společenských zájmů, které chrání Trestní zákon - za jeden skutek se dají považovat různá stádia vývoje trestné činnosti (příprava, pokud, dokonání TČ) - jeden skutek může mít znaky více trestných činů a nebo žádného - né každý skutek je tedy třestným činem - skutek se TČ stáva pokud naplní znaky skutkové podstaty některého trestného činu uvedeného v Trestním zákoně (TZ) - na základě skutku OČTŘ prvně rozhodnou, zda se vůbec jedná o trestnou činnost - pokud ano, tak zahajují trestní řízení/stíhání - pokud ne není dále co řešit.

Právní kvalifikaci chápeme jako subsumpci/zařazení skutku pod příslušné ustanovení TZ nebo jiných předpisů z oboru trestního práva

4.3 Trestný čin

§13 TZ - říká, že TČ je to co TZ popisuje jako TČ - čin který naplňuje znaky skutkové podstaty některého z TČ popsaných v TZ - k trestní odpovědnosti je potřeba úmyslného zavinění nestanoví-li zákon výslovně, že stačí zavinění z nedbalosti - už máme pouze formální pojetí TČ (problém pro etické hackery) - dříve formálně-materiální pojetí (společenská škodlivost)

Prvky trestného činu:

- **objekt** (co je chráněno TZ | předmět je to na co útočí)
- **objektivní stránka** (popis co bylo spácháno a jaké to mělo následky + vztah mezi jednáním a následkem-příčinný vztah - kauzální nexus) - obligatorní znaky: jednání, následek, kauzální nexus(příčinný vztah) - fakultativní znaky: místo, čas a způsob jednání - na fakultativní znaky se musí ohlížet (některé TČ jsou jimi jen na nějakém místě v určitém čase nebo určitým způsobem jednání) můžou zapříčinit že daný skutek není TČ - Objektivní stránka nejzřetelněji odlišuje různé typy trestného jednání
- **subjekt** (kdo je pachatelem) - určen: věkem, příčetností, způsobilostí, postavením
- **subjektivní stránka** (zavinění, vztah subjektu k TČ | úmysl, nedbalost)

4.3.1 Souběh TČ

spáchání více TČ najednou (dřív než je jeden z nich odsouzen rozhodnutím soudu 1. stupně).

- **Jednočinný souběh** (též konkurence trestních zákonů) – stav když je více TČ spácháno (konkurence více právních kvalifikací) nad jedním skutkem (jedním skutkem/činem)
- **Vícečinný souběh** – souběh/konkurence více TČ nad více skutkami
  - stejnorodý (stejné skutkové podstaty/stejné TČ)

- nestejnorodý (různé skutky podstaty/ různé TČ)
- kombinace:
  - jednočinný stejnorodý
  - jednočinný nestejnorodý
  - vícečinný stejnorodý
  - vícečinný nestejnorodý

Obecně se tresty TČ nesčítají (tomu tak je v USA, u nás ne) - posuzovat souběh je důležité, aby obviněný nebyl trestán víckrat za jeden skutek pokud je jejich souběh vyloučen (zajištění aby pachatel nebyl potrestán dvakrát za stejný čin)

4.3.2 Úhrný a souhrnný - úhrný trest

Za jeden čin/skutek můžeme být potřestaný více skutkovejma podstatama - proniknu k poč. systému a tam získám udaje díky kterým padělám platební prostředek - trestá se podle závažnější skutkové podstaty a drží je horního limitu trestu a dá se i trošku navýšit - zajištění aby pachatel nebyl potrestán dvakrát za stejný čin - souhrný trest je když sem odsouzený za jeden TČ a pak jsem odsouzenej za další tak se dělá sourhný trest kde se zase posuzuje ten závažnější TČ - obecně se tresty TČ nesčítají (tomu tak je v USA, u nás ne, u nás se používá úhrný a sourhný trest)

4.4 Postup pri kvalifikaci trestné činnosti

- Podnět -> přípravné fáze -> Rekognoskační fáze (jde opravdu o TČ?) -> zahájení vyšetřování -> vyšetřování el. místa činu -> vyšetřování fyzického místa činu -> zpracování důkazů -> dokazování před soudem
- **Zánik trestní odpovědnosti** - Účinná lítost - Promlčení (20 let, 15 let, 10 let, 5 let, 3 léta) - Vyloučení z promlčení
- police zajišťuje informace vedoucí ke kvalifikaci trestného činu a identifikaci pachatele

Zásady jurisdikce:

- zásada teritoriality - TČ v ČR
- zásada registrace - TČ na plavidlech, letadlech registovaných pod ČR (pod českou vlajkou)
- zásada personality - aktivní - TČ spáchaný českým občanem - pasivní - TČ spáchaný na českém občanu
- zásada ochrany a univerzality - obecné zásady - okrajové prinicpy (moc nenastávají) - třeba když někdo páchá genocidu tak je to stíhatelné podle práva ČR vždycky, bez ohledu na to kde je to páchané
- Spáchání:

  - Úmysl
  - Nedbalost
- **Formální pojetí TČ** - tč je to co je napsáno v TZ není potřeba škodlivosti/protiprávnosti
- Prípravné řízení -> předběžné projednání obžaloby -> hlavní líčení -> odvolací řízení -> výkon rozhodnutí
- Podezřelí -> obviněný (oznámení obvinění / zahájeno TŘ) -> obžalovaný (podání obžaloby státním zástupcem k soudu) -> odsouzený (soud rozhodl o vině a trestu)
- Trestní právo hmotné -> Skutkové podstaty -> trestné činy (trest)

Ke klasifikaci každý přistupuje trochu jinak (otázka 5).

5 Kategorizace kyberkriminality (včetně příkladů trest-né činnosti v jednotlivých kategoriích)

Kyberkriminalitu je možné kategorizovať z niekoľkých rôznych hľadísk.

1. Obecne je kyberkriminalitu možné kategorizovať:

– podľa trestného práva hmotného
– prostredníctvom klasifikácie bezpečnostných incidentov

2. Pomocou využitia **taxonomie** sa kategorizuje podľa prístupov:

– Klasifikácia podľa CIA triády
– Klasifikácia podľa charakteru útočníka
– Klasifikácia podľa charakteru útoku

3 Kategorizácia podľa UNODC:

– Útoky na CIA triádu - MITM, DoS...
– Trestné činy súvisiace s počítačom - spamming, vydieranie, zneužitie identity...
– Trestné činy súvisiace s obsahom - detská pornografia

4. Kategorizácia podľa využitia ICT prostriedkov:

– **Cyber-dependent** - páchaná jedine prostredníctvom ICT. Kategóriu je ďalej možné rozdeliť na
  – činy ohrozujúce CIA triádu
  – využívajúce ICT
– **Cyber-enabled** - tradičné činy páchané prostredníctvom ICT
– **Cyber-supported** - Incidentálne využitie ICT (byli použity ICT a tak vznikají el. důkazy (telefonování))

5.1 Taxonomie

– Stromová klasifikace pojmů - sdružuje skupiny incidentů a přiděluje jim skudkové podstaty odpovídající právní úpravy.
– ENISA/EUROPOL taxonomie - klasifikace podle charakteru útočníka a útoku
– Česká taxonomie dělení do skupin (Sběr informací, škodlivý kód, pokus o průnik, průnik, podvod) - v nich jsou definovány škodlivá jednání - klasifikace podle TZ v případě, že ji lze považovat za TČ - spam a scaning nejsou standardně trestné, ale za určitých podmínek už ano (spam s poplašnou zprávou nebo phishingem - taxonomie zároveň popisuje návody pro postup při výskytu určitého incidentu.

– OSN - UNODC - organizace OSN pro organizovaný zločin, kategorizace nic moc, prolínají se kategorie - Útok na CIA (hacking, MitM, DoS) - Trestné činy související s počítačem (Podvod, vydírání, zneužití identity, spamming, duševní vlastnictví, poškozování osob a skupin) - Trestné činy související s obsahem (Dětská pornografie)

5.2 Cyber-dependent

– **Porušení tajemství dopravovaných zpráv (§182 TZ)** - útok na důvěrnost - i klasická pošta, email, neveřejný přenos počítačových dat. 3 roky vězení max, Zneužití pracovní pozice, např že jsem ISP tak je to kvalifikovaná TČ až 5 let, MitM
– **Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§183 TZ)** - neoprávněné porušení tajemství - Kámoš nahlédne do mé soukromé složky, dokumentů
– **Neoprávněný přístup k počítačovému systému a nosiči informací (§230)** - 2 skutkové podstaty v jednom
  – neoprávněné překonání bezpečnostního opatření -> získá přístup k počítačovému systému a tým spáchal trestný čin (CZ.NIC se skenoval síť proti defalutním nastavením kamer, ale tím páchali TČ. Když vím jaké heslo má kamarád a nebo mi ho klidně i řekne ale nedovolí mi se k němu připojit a já se připojím tak páchám TČ) = 2 roky
  – po neoprávněném získání přístupu padělání nebo pozměnění dat = 3 roky -> úmysl omezit fungování (4 roky), pokud je to právnický subjekt, státní správy, podniku nebo státní moci (5let)
– **Opatření a přechování přístupového zařízení a hesla k počítačovému systému a jiných takových dat (231 TZ)** Příprava hackingu je TČ - má to vlastní skutkovou podstatu, aby mě mohli potrestat když to budu připravovat někomu jinému - pokud je to pro výskum tak to trestné není.
– **Požkození záznamu v počítatčovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§232 TČ)** - pro profesionály - někdo odpovědný za bezpečnost a chová se drubě nedbale a způsobí to značnou škodu (>500 000) je to TČ - max 6 měsíců.
– **Neoprávněné opatření, padělání a pozměnění platebního prostředku (§234 TZ) - phishing do bank a platebních kare**t - trestná i příprava - získání něčích údajů a pak s nima dál nakládám (2 roky) - padělání (5 let) - sám použiju pro své obohacení (8 let).
– **Výroba a držení padětelského náčiní**

5.3 Cyber-enabled

– **Výroba a jiné nakládání s dětskou pornografii (§192 TZ)** - bez distribuce el. sítí (2 roky) - šíření ručně (3 roky) - šíření el. sítí (6 let)

- **Porušení autorského práva (§270 TZ)** - prostřednictví počítačové techniky je to horší
- **Nebezpečné pronásledování (§354 TZ)**
- **Podvod (§209 TZ)** - phishing, sociální inženýrství, často spojené s něčím jiné propagace drog, hanobení národa apod. - kvalifikovaná podstata jiných TČ

6 Kyberkriminalita v užším smyslu slova (příklady trestné činnosti a kvalifikace dle zvláštní části TZ)

Kyberkriminalita – v užším smyslu do něj zahrnujeme **trestnou činnost**, která směřuje právě přímo proti důvěrnosti, dostupnosti, či integritě informačních systémů (neoprávněný přístup k počítačovému systému a nosiči informací, nebo opatření a přechovávání hesla a přístupového zařízení k počítačovému systému).

6.1 Příklady trestné činnosti

- **Scanning** - pouze pokud je to prováděno na účelem následného zneužití (§230, §182) - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat §231
- **Sniffing** - Poručení tajemství dopravovaných zpráv §182 - Příprava nástrojů §231 - Neoprávněné opatření, padělání a pozměnění platbního prostředku §234
- **Phishing** - Příprava nástrojů §231, získání např přístupových údajů za účelem §230 nebo §182 - Podvod §209 - Platební prostředky §234
- **Ransomware** - Podvod §209 - Neoprávněný přístup §230 - Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí §183
- **(D)DoS** - Neoprávněný přístup §230 - jsou tam na to speciální písmena - v DDOS ještě další §230 aby získal botnet - teoreticky i §231 příprava nástoje pro následující útok
- **Využívání zranitelnosti/exploitu** - §230 při dokonání - §231 při neúspěšném pokusu je stále dokonaná příprava (musel si ten exploit připravit) takže kvalifikace podle §231

7 Elektronické důkazy a jejich specifika v trestním řízení.

Základní specifika/problémy:

- Neexistuje specifická úprava pro práci s el. důkazy -> používají se standardní nástroje TP procesního
- Nutnost přenesení důkazu do vnímatelného zachycení, aby se sním mohl seznámit soudce - el. důkazy se těžko převádí do vnímatelného zachycení - např dokazování zdrojovým kódem nebo metadaty se nedá jentak samo použít - soudce by nevěděl do čeho kouká - nutnost interpetace
- Nedostatek/absence obecně uznávaných postupů - ani judikatura (soudy moc ještě nerozhodovali o specifikách el. důkazů) - OČTŘ nemá jasně definovaný postup jak s el. důkazy nakládat - na různých úrovních nebo v ruzných krajích se to dělá jinak
- volatilita el. důkazů - rychle se menící prostředí - data mohou mizet - proto máme nástroj freezing
- často přeshraniční charakter
- nedostatek vzdělaných lidí, znalci, zástupci, soudci - předpokládá se vyšší úroveň zločinců(chytřejší, organizovanější), než jen ty co se vloupávají do chat apod

Základní zásady dokazování = presumpce neviny - zásada ústnosti (ústně a prezenčně se důkazy předávají soudci a osvšem okolo, problém s el. důkazy) - **zásada veřejnosti - zásada bezprostřednosti** (soudce je seznámen s důkazy bezprostředně, problém s el. důkazy, né všechno se dá přinést k soudu, potřeba vymyslet mechanizmus jak soudce co nejbezprostředněji s důkazem seznámit) - **zásada materiální pravdy - zásada vyhledávací - zásada volného hodnocení důkazů** (neexistuje dělení důležitosti důkazů, vždycky je to subjektivní hodnocení, problém s el. dukazy, když soudci někdo pořádně nevysvětli jak byl důkaz vygenerován, co to znamená a jak je to spolehlehlivé je to pro něj vělmi těžké volně hodnotit a tak může kvalitní el. důkaz diskreditovat) - **zásada zdrženlivosti** (redukce škod, například při zajišťování důkazů při domovní prohlídce)

7.1 Důkaz

Jakákoliv informace, kterou získáváme - vyvracuje nebo potvrzuje skutkovou okolnost - může to být cokoliv co může přispět k objasnění věci - není nikde definované co to může být.

Musí být získán **zákonným postupem** (získán důkazním prostředkem).
Dokazuje se:

- zda se stal skutek, který považujeme za TČ - kdo ho spáchal (zda to byl obviněný)

– z jakých pohnutek (důvodu), aby se dalo rozhodnout jestli skutek nenaplňuje kvalifikovanou skutkovou podstatu
– následky TČ (co bylo napácháno za škody a že je mezi nimi kauzální nexus) - poměry obviněného - okolnosti vedoucí ke spáchání nebo okolnosti (spolupachatelné, nedbalosti apod)

Dělení důkazů:

– Osvědčující X Vyviňující
– Původní X Odvozené - svěděk, který to viděl (původní) - svědek, který se o tom od někoho dozvěděl (zprostředkovaný svěděk/důkaz | Odvozený)
– Přímé X Nepřímé - příme vypovýdají o zkutečnosti, nepřímé je že se někdo z daného počítače připojoval k serveru, ale přímo se neví (musí se dávat do souvyslostí, víc nepřímích)

U každéno důkazu se posuzuje jeho důkazní moc (síla) a to v podobě volného hodnocení důkazů Složky:

– **Závažnost důkazu** - do jaké míry dokazuje přímo či nepřímo danou skutečnost
– **Pravdivost důkazu** - důvěryhodnost zdroje důkazu, jak moc se můžeme spolehnout na pramen důkazu a na spolehlivost získání důkazu - analýza dat pomocí AI (každý přisoudí subjektivně jinou pravdivost/věrohodnost)
– **Zákonnost důkazu** - zde už spíše objektivně:
  – zda byl důkaz zajištěn v souladu s příslušnými předpisy (zda nebyl získán protiprávně) -> jakýkoliv protiprávní prvek při získání může vést k jeho neplatnosti (např pokud by policie daný pramen důkazů ukradla (telefon))
  – úkon musí být proveden oprávněným subjektem - zda existuje vztah důkazu a skutku - zda byl zajištěn přípustným způsobem (nepřípustný důkaz = nesmí se k němu přihlížet, ani OČTŘ ani pak soudce, jako kdyby neexistoval)
  – Podstatné X Nepodstatné vady – některé vady jsou opravitelné (napravitelné X nenapravitelné vady)

    Odposlech na základě soudu nebo na základě souhlasu účstníka komunikace, ale souhlas musí být protokolovaný, pokud není protokol, tak je důkaz neplatný dokud ho nedoplním - **Doktrína otráveného stromu** (hlavně v USA), všechny navazující důkazy jsou neplatné (odposlechem zjsitím heslo a pomocí toho se dostanu k něčemu = neplatné všechno), u nás to není tak striktní, ale furt to není vyřešené jak moc to platí nebo ne

Vyhledávání důkazů (často předchozí důkazy, provozní a lokalizační údaje mi řeknou kde zdroj) -> Procesní zajštění důkazního materiálu (nejproblematičtější z hlediska generování zákonných důkazů) -> prověrka (získání důkazu z důkazního materiálu/pramene

důkazu) -> volné hodnocení (jak OČTŘ i soudce, zda je zákonný, pravdivý)
Procesní zajištění důkazů - musí nejprve zohlednit 2 věci - charakter důkazu(dat X hardware apod) - odkud budou zajišťována - na základě těchto 2 kritérii je zvolen procesního prostředku (nástroje) - musí se zohledňovat základní zásady dokazování (přiměřenost postupu - pokud můžu získat důkaz procesně složitějším způsobem, ale který zasahuje míň do práv, musím zvolit ten který zasahuje méně - nedělat odposlech/domovní prohlídku pokud to jde jinak)

7.1.1 Zajištění el. důkazů

- **Zajištění zařízení či datového nosiče (získám hardware a tím se dostanu k el. důkazům)** - Vydání a odnětí věci - osobní prohlídka - domovní prohlídka a prohlídka jiných prostor -ohledání věci
- **Přímý přístup k datům prostřednictvím (třeba počítačové sítě, nebo telefon přijonená někam)**
  - Orgány můžou přístoupit k lokálním datům přímo bez souhlasu, pokus jsou data součástí odňatej věci
  - Orgány můžou přístoupit k vzdáleným datům přímo bez souhlasu, pokud znají přístupové údaje (našli je napsané nebo od manželky), potřebný souhlas soudu
  - K datům na připojených službách:
    - Podle postupu §158 odst. 3 (Sledování osob a věcí) – aktuální data (nutné pořídit protokol k dokazování)
    - Podle postupu §88 (Odposlech) – budoucí data

    V obou případech je taktéž potřebný souhlas soudu
- **Přístup prostřednictvím držitele/správce dat** - požádání toho kdo je má v držení nebo je spravuje aby mi ty data zpřístupnil nebo dal - obecně mě to mají povinnost vydat - specificky pak potřebuju odposlech nebo sledování.

  Data od ISP
  - provozovatele podle Zákona o elektronických komunikacích (provozovatele sítí,operátoři) - provozovatele obvykle žádná data neuchovávají, ale podle data retention musí uchovávat metadata (provozní a lokalizační údaje) a poskytnout odposlech
  - provozovatele podle Zákona o některých službách iformační společnosti (poskytovatele služeb na internetu (FB, google, seznam))
- Podle charakteru dat se používají následující procesní postředky:
  - Dožádání (obecná součinnost) – nelze stáhnout na utajované -osobní údaje, údaje uchovávané v soukromí, metadata, obsahové data komunikací protože mají specifickou úpravu
  - sledování osob a věcí pro data uchovávaná v soukromí (data hosting)

– data retention pro zajištění metadat – útvar zvláštních činností na základě rozhodnutí/příkazu soudu, operátor/poskytovatel služby musí tyto provozní a lokalizační data uchovávat půl roku
– odposlech pro přenášení/komunikační data – realizován útvarem zvláštních činností -soud na základě zádosti státního zástupce vydá rozhodnutí o odposlechu, jakákoliv služba (ne jen telefon, email ale i sledování kom. PC nebo sledování účtu a sledování přibývajících ubývajících dat), max 4 mesíce, pokud souhlas uživatele, tak není potřeba souhlas soudu, vypracovává se protokol, z hlediska procesního práva policii nic neprání v tom se do komunikace vbourat např do zašifrované, odposlech možný i dobudoucna (i když neví zda TČ probíhá) musí to však být stále dobře odůvodněné
– freezing (zamražení dat) – aby nebyla zneužívána volativita el. důkazů, utajované pro uživatele, max 90 dní

7.1.2 Hodnocení a provedení důkazu

Jedná se o poslední klíčovou fázy v procesu dokazování - důkaz musí být **smyslově vnímatelný** pro soudce (velký problém při el. důkazech) a musí jednoznačene/dostatečně/srozumitelně vypovídat o skutečnsoti kterou má dokazovat.
Při dokazování datama se proto využívají interpretační prostředky (data uložená na disku mi jsou k ničemu pokud nemám interpretační prostředek, který mi je zobrazí do vnímatelné podoby) - např když dokazuji kódem, tak jako interpretační prostředek použiju znalce, který vysvětlí co v tom kódu je a co dělá, nebo kód zkompiluju a dokazuju vzniklím počítačovým programem nebo webovou stránkou apod - pokud dokazuju datama v určitém datovém formátu, potřebuju sofwarové/harwarové vybavení, které ty data interpretuje do srozumitelné, člověkem vnímatelné podoby - to je zase problém protože když budu mít nějaký proprietární firmware čipu z auta třeba, tak pro interpretaci budu potřebovat specifický forenzní nástroj nebo to potřebuju nějak nainstalovat do toho auta a to přinést k soudu :) - pak se musí dokazovat i že ten interpretační prostředek interpretuje správně a nebo to to co vzniklo kompilací kodu dělá to co autor původně zamíšlel - třeba webové stránky se mohou na každém PC chovat jinak - interpret to tak pak může zkreslovat, ale soudy se k tomu zatím moc nevyjádřili.

Často se řeší **znaleckými posudky** - odborníci v oboru s technickým vybavením - snaží se vysvětlit/odpovědět na technické otázky u soudu - dostane počítač a otázka je zda na tomto počítači prokazatelné že uživatel páchal TČ - znalec odpoví ano nebo ne a odůvodní odpověd s důkazy - jmenuje to předseda soudu - není zádná znalecká komora - není žádná certifikace znalostí/ odborné způsobilosti - znalci se vyjádřují k právním otázkám - často se stává, že soudy ani neumí formulovat zadání znaleckého posudku - v tom případě se spolupracuje se znalci na formulaci otázky, na kterou pak odpovídají (potenciálně problematické).

provedení důkazu - bezprostřednost, ústnost, veřejnost - často se předčítají znalecké posudky a jiné důkazy - často se znalec musí učastnit soudu, bývá vyslýchaná a doptávají se ho na další detaily - obecně je problém že se to tak musí dělat a v soudních síně nedisponují dostatečnou technikou na interpretaci, nebo nelze tam přijet s autem (příklad s čipem v autě) - takže se to obvykle řeší znaleckými posudky

7.2 Důkazní prostředek

Prostředky pomocí kterých můžeme zjistit stav věci - to co může u soudu reprezetnovat důkaz ve smyslově vnímatelné podobě - výsledek procesního postup OČTŘ při zajišťování důkazů - např výslech svědka, znalecký posudek - obecně to může však být cokoliv

7.3 Pramen důkazu

Věc, ze které je důkaz čerpaný - např datový nosič, PC, dokument, metadata dokumentu, software, softwarové logy, hardware

8 Procesní nástroje pro zajišťování elektronických důkazů.

8.1 Obecná součinnost §8

Státní orgány, fyzické a právní osoby a další relevantní subjekty mají povinnost vyhovovat na dožádání - OČTŘ chce informaci a tak provede dožádání a daný subjekt by na tuto žádost měl vyhovět - pokud existuje specifická právní úprava musí se použít ta - plus soudy pak řeší proporcionalitu se zásahem do práv suběktu - zjišťování nejzákladnějších informací (obvykle v rekognoskační fázy) - pro utajované informace je potřeba příkaz(souhlas) soudce (§8/5 "paragraf 8 odstavec 5)

8.2 Freezing §7b

Vyžaduje to po nás Úmluva o kyberkriminalitě - 2 procesní nástroje

- *freezing* – hrozí ztráta zničení nebo pozměnění dat důležitých pro třestní řízení, lze nařídít osobě která je drží, aby je uchovala v nezměněné podobě pro potřeby dálšího vydání vyšetřovatelům (při phishingu zamrznutí nasbírané databáze)
- *blocking* – příkaz na provozovatele služby, aby zablokoval přístup užívatele k daný datům (max 90 dnů), poskytovately služby (ten kdo freezing provádí) musí být vysvětleno co má být zmraženo, proč a na jak dlouhou dobu

8.3 Odposlech a záznam telekomunikačního provozu §88

při vedení TŘ pro zločin s odnětím svobody min. 8 let nebo pro vyjmenované TČ nebo pro umyslné TČ k jehož stíhání nás zavazuje mezinárodní smlouva

- může být vydán příkaz (úkon) pro zajištění obsahu telekomunikačního provozu (tekoucí data, e-maily telefonáty) - zajištěno **Útvarem zvláštních činností**
  - mívají nainstalované zařízení, které umožnuje tento odposlech
  - odposlech realizují ve spolupráci s operátorama a ti za to dostávají peníze
- pokud nelze sledovaného účelu dosáhnout jinak nebo pokud by to bylo moc složité (preferují se jiné úkony) - potřeba příkaz soudu - nebo i bez soudu se souhlasem uživatele - odposlech možný vydat i dobudoucna (i když OČTŘ neví zda TČ probíhá) musí to však být stále dobře odůvodněné

8.4 Zajištění provozních a lokalizačních údajů §88a odst. 1

metadata k tekoucí komunikaci - na základe příkazu soudu - pokud úmyslný TČ min 3 roky nebo vyjmenované nebo TČ vyhlášený mezinározní smlouvou - pokud učelu nelze dosáhnout jinak - nutno zajistit aby tyto údaje byly uloženy poskytovatelem - na to máme úpravu Zákona o elektronických komunikacích

8.5 Data retention §97 - Zákon o elektronické komunikaci (ZoEK)

ZoEK říká co jsou provozní a lokalizační údaje:

- **metadata o komunikaci** - údaje by neměli nic říkat o přenášených datech (poskytovatel by třeba měl odfiltrovat data obsažená v URL třeba z formulářů)
- poskytovatel je na základě data retention povinen uchovávat provozní a lokalizační údaje po dobu 6 měsíců od doby uskutečnení daného komunikačního provozu (za to poskytovatel dostává peníze), nesmí být poskytovatelem zneužita. Pokud nejsou po 6 měsících vyšetřovately požadovana musí je tekomunikační operátor zkartovat

8.6 Sledování osob a věcí 158d trestního řádu

Pátrací prostředek - primárně určen pro zajištění operativních informací -> zjistit co se stalo, ale jé na zjištění důkazů pro soud (tak tomu bylo původně)

Pokud chci zjištěné informace použít jako důkaz u soudu musím o tom vypracovat protokol - dnes se to používá i pro zajištění el. dat jako důkazů. Postup:

1. vyšetřovatel potřebuje data z uložiště -> zahájím sledování osob a věcí
2. jako součinnost si vyžádám spolupráci od poskytovatele služby, který data uchovává -> a v rámci té součinnosti mi poskytně i ty data, která chci
3. když udělám protokol o tom jak jsme získal danou spolupráci, kdo mě poskytnul součinnost, jak jsem postupoval a jaká data jsem získal -> mužu daná data použít jako el. důkaz u soudu

O vydání příkazu o sledování osob a věcí rozhoduje státní zástupce prostřednictvím povolení - pokud jsou to ale soukromá nebo utajovaná data je potřeba předchozí povolení soudce - dá se udělat neodkladný úkol (získám telefon a neodkladně se kouknu na data uložená na vzdálené službě) pokud pětně bude soud souhlasit.

8.7 Domovní prohlídka a prohlídka jiných prostor

Postup:

– Soudce vydá příkaz k realizaci domovní prohlídky
– policejní orgán tam provádí ohledání věcí relevantní k trestnímu stíhání - policejní orgán musí soudci dostatečně vysvětli proč se domnívá že v příslušných prostorách jsou veci důležité pro TŘ
– soudní zástupce sepíše podání na soud ve kterém žádá o vydání příkazu k domovní prohlídce ve které uvede co je cílem a proč a proč si myslím že to tam bude a oduvodním že to nejde jiným nástrojem
– soud to posoudí a v rámci rozhodnutí pak vypíše informace na základě kterých se rozhodoval a tím oduvodní vydání daného příkazu - nedá se odvolat, ale stát ručí za škody způsobené nesprávným vydáním příkazu o domovní prohlídce

Procesní podmínky za kterých může být domovní prohlídka realizovaná:

– přiměřenost - odborná péče buď vyšetřovatel nebo znalec (když to dokážou ohledat na místě nemusí se to odvážet)
– potřeba přítomnosti majítele prostor nebo musí být aspoň informován o tom co se tam děje
– nezúčastněná osoba (někdo externí, soused) kdo zkontroluje že nedochází k porušení zákona při prohlídce
– vypracovává se protokol (videozáznam, foto) - všichni kdo se zučastní ho podepisují i nezúčastněná osoba

Aby přistihly zločince se zapnutím PC a přihlášením do vzdálené služby - dá se přizvat znalec pro specifickou činnost se specifickým vybavením - musí se dodržovat specifické postupy aby nebyly důkazy znehodnocovány - zapečetění, zabalení do pytle za přítomnosti nezúčastněné osoby.

8.8 Výdání a odnětí věci

Nástroj pro zajištění věci od člověka - každý má Ediční povinnost (na požádání musí vydat drženou věc) - OČTŘ ho vyzvou k předložení věci - pokud odmítně věc vydat může mu být odejmuta (pořádkové opatřené) stačí rozhodnutí státního zástupce - při odejmutí věci by měla být přítomna nezúčastněná osoba - pořizuje se protokol - osobě se dá potvrzení o odejmutí - pokud jsou na zařízení data o kterých je povinná mlčenlivost (utajované informace, advokátní tajemství) je specifický postup - pouze věci né data - ovšem pokud je vydán např telefon tak naněm může být provedena forenzní analýza a tedy je možno se dostat k datům uloženým na zařízení

8.9 Osobní prohlídka

domnívám (jako OČTŘ) se že daná osoba má u sebe věc důležitou pro TŘ, ale nevím to jistě -> zahájím osobní prohlídku - na základě rozhodnutí soudu nebo státního zástupce - pokud je to neopakovatelný úkon můžu osobní prohlídku provéset i bez příkazu (zatknu osobu co utíká z místa činu a mám podezření že u sebe má zbraň se kterou páchal TČ) musím pak ale souhlas zpětně získat - je to zhojitelná vada neučinného důkazu - úkonu by měl předcházet předchozí výslech (jako u domovní prohlídky) což bych osobu měl požádat zda věč/předmět u sebe má a zda mi ho nevydá.

8.10 Ohledání věci

pozorování a sbírání informací za účelem objasnění věci - protokol co bylo vypozorováno a jak - typicky při domovních a osobních prohlídkách - na místě najdu spuštěný počítač a na místě chci provést jeho ohledání - v takovém případě s kamerou nebo foťákem provádím záznam toho co jsem objevil.

Nemůžu provést obecné ohledání věci - např. když ohledávám na místě zaplé PC a bude tam probíhající komunikace a já bych ji chtěl sledovat (odposlech má větší zásah do práv), tak to nemůžu udělat jen na základě ohledání věci (generovalo by to neúčinný důkaz) - avšak policie si proto může předem připravit příkazy- například existují příkazy k domovní prohlídce, odposlechu a sledování osob a věcí a tím pádem může získávat všechno na místě.

9 Specializované útvary OČTŘ ve vztahu ke kyberkriminalitě.

9.1 Policie ČR

- **Policejní presidium** -> Skupina informační kriminality - dřív více - hlavní organizační prvek Policie ČR - koordinace a metodika - cílení na konzistenci pri vyšetřování.
- **Odbor kriminalistické techniky a expertíz (OKTE PČR)** - znalecký ústav - akreditace na digital forensics (získávání el. důzaků z dat) - znalecká činost - zpracování znaleckého posudku - málo lidí a tak tyto služby nabízí soukromnící kteří jim tyto služby prodávají (komerční činost).
- **Kriminalistický ústav Praha** -> Oddělení počítačové expertízy - také znalecká činost ale jako externí služba
- **Útvar zvláštních činností Policie ČR (UZČ SKPV PČR)** - centrální útvar policie v Praze - expozitůry v jednotlivých krajích - poslituje vyšetřovatelům služby - odposlech a zajišťování dat od poskytovatelů a poskytovatelů služeb (provozní a lokalizační údaje) - má k tomu kontaktní sítě a vybavení - vyšetřovatel požádá soud o příslušný příkaz, ten dá utvaru zvláštních činností, který daný úkon provede (zajístí odposlech, zajístí data) a pak je v protokolu předává - často postupují striktně podle zákonného postupu a tím se proslužuje doba vyšetřování
- **Národní centrála proti organizovanému zločinu** - spojením útvaru pro odhalování organizovaného zločinu a útvaru pro odhalování finanční kriminality - vyšetřování nejzávažnějších druhů kriminality - včetně rozsáhlých kybernetických útoků (rozsáhlé ransomwéry, útoky na kritickou infrastrukturu) - expozitury v jednotlivých krajích - 2 role - vyšetřování - vytváření metodiky pro ostatní vyšetřovatelé/útvary policie (jaké techniky, jaké nástroje používat při vyšetřování)
- **Analogická pracoviště na krajských ředitelstvích PČR (oddělení kybernetické kriminality, odbor poč./inform. kriminality)** - různé jméno v různých krajích - vyšetřování na lokální úrovni - neúspěšnější jihomoravský kraj, snaží se předávat znalosti do ostatních krajů
- **Europol -> EC3 jednotka** - Evropské centrum pro boj proti kyberkriminalitě - metinárodní - nevyšetřují - podávají metodiku - sestavují mezinárodní týmy
- **Evropská agentura pro bezpečností sítí a informací** - ENISA
- **specializovaná pracoviště na Interpolu** - mezinárodní - nevyšetřují - podávají metodiku - sestavují mezinárodní týmy

9.2 Státní zastupitelství

neexistují zvláštní specifické instituce/zástupci - pouze neformální skupiny na urovní nejvyššího státního zastupitelství nebo na úrovni krajského státního zastupitelství - předávání metodiky a snaha o zajištění koordinace a vzdělávání obecne vělký problém nevzdělanosti - neexistuje jak je donutit se vzdělávat - dělají to dobrovolně

9.2.1 Nejvyšší státní zastupitelství (NSZ)

významná role, že může vydávat metodická opatření - dokumenty doporužující metodiky jak by se mělo co dělat

metodický pokyn 1.2015 - popisuje, který procesní nástroje na které el. důkazy

9.2.2 Justiční akademie

příspěvková organizace státu - poskytuje nadstandardní vzdělávání soudům a státním zastupitelstvím

Školení NÚKIB - semináře NSZ - akademická sféra - Ústav pro kriminologii a sociální prevenci, úzká vazba na ministrestvo spravedlnosti a na nejvyšší patra policie (zatím jen statistické studie)

9.3 Soudy

neexistují ani neformální skupiny

10 Mezinárodní spolupráce v oblasti kyberkriminality.

Problémy:

- neharmonizovaná legislativa - využívání bezpečných přístavů - negativní kolize - kyberprostor nemá hranice ale právo jo
- složitá a pomalá harmonizace - chceme aby se harmonizace dotýkala co nejvíce států ale o to těžší je se dohodnout na slopečné věci
- Neochota některých států spolupracovat - fragmentace internetu - nebo některé státy nejsou dostatečně vyspělé a nemají lidi na to aby spolupráci poskytli
- pomalá spolupráce - obecné poskytnutí spolupráce (MLA) trvá příliž dlouho k volatilite el. důkazů a státy nemusí spolupráci vůbec přijímat - pachatel se může rychle přemisťovat (i se serverem)
- neexistence nástroje pro el. předávání důkazů

Právo je teritoriální - každý stát vykonává svou suverenitu na svém území - snaha o mezinárodní harmonizaci/standardizaci - ale státel právo platí lokálně (omezeně teritoriálně pravomoci OČTŘ). Teritoriální charakter práva nesedí s charakterem informačních sítí - geolokace a georestrikce funguje spíše v soukromoprávních vztazích (Neftlix nabízí ruzné filmy pro ruzné státy).

Většina kyberkriminality má přeshraniční prvek - nekdě je přeshraniční prvek natolik velký že se jim OČTŘ musí zabívat - pachatel a poškozený v jiných státech - pachatel a poškozený ve stejných státech ale vetšina dat souvsejících s TČ (důkazu) je v zahraničí - často to má dopad na výsledek TŘ (získání důkazu trvá nebo se k nim nelze vůbec dostat apod) - při přeshraničním charakteru klesá účinnost vyšetřování.

Často hrají velkou roli i zahraniční poskytovatelé služeb (ne jen stát), to má zase jiný charakter ne jednání státu se státem.

Hlavní právní problémy - podle kterého práva? - co je a není trestný čin? - kdo a jak má získávat důkazy a provádět úkony a jakým způsobem? (Policie ČR nemuže provádět úkony v zahraničí) - jak spolupracovat?

10.1 Podle kterého práva

- **suverenita** – právo státu vykonávat státní moc nad určitým územím (teritorium, stát, lodě, vzduch)
- **jurisdikce** - právo státu definovat povinnosti a práva lidí - státy se obvykle staží rozšířit svou jurisdikci

– **rozhodné právo** - pravidla která říkají že na určitý případ se vztahuje určité právo (komu to spadá do jurisdikce) -> do určité míry mezinárodními úmluvami - vetšina států má jimi implementovanou jurisdikci ve svém právním řádu (problém je s výkladem, i když to mají implementované stejně tak dochází ke problémům)

V soukromém právu si můžeme zvolit podle kterého práva chceme postupovat a soud pak podle něj soudí - ve veřejnoprávních odvětvích jako je trestní právo to tak není - když určíme že v nějakém případě platí právní řád nějakého státu, začnou to řešit/rozhodovat orgány daného státu a to dělají podle jejich práva, né jiného (nemůžou si vybrat).

Vymezení jurisdikce ČR na základě principů:

1. **princip teritoriality** – vztah k prostoru ČR -> např v jednom státě může být provozován malitious server, v druhém může být skupina lidí koordinující útok a ve třetím státě muže být dopad útoku (všechny tři státy si mohou nárokovat jurisdikci podle principu teritoriality)
2. **pricip personality** – aktivní (občan ČR spáchal) a pasivní (vůči občanu ČR byl ospácháno)
3. **princip registrace** – letadla a plavidla pod vlajkou ČR spadají pod jurisdikci ČR
4. **pricip ochrany a univerzality** – obecné principy, okrajové principy (moc nenastávají) -> třeba když někdo páchá genocidu tak je to stíhatelné podle práva ČR vždycky, bez ohledu na to kde je to páchané - požádání cizého státu který na má připad v jurisdikci aby byl případ odtíhán ČR tak se to bude řešit podle Českého práva

Z těchto principů je vidět že jurisdikci nad určitým prípadem si může nárokovat více států najednou (kolize jurisdikcí) - kolize jurisdikcí se řeší z pravidla domluvou nebo to řeší nějaká mezinárodní organizace - určí si kdo to bude stíhat, nebo založí společný vyšetřovací team a stíhají to ve spolupráci v obou státech. Může vzniknout:

– pozitivní kolize (více státu si nárokuje jurisdikci)
– negativní kolize (nikdo si nenárokuje jurisdikci)

Pachatel muže distibuovat svou činost tak aby to co zrovna páchá v konkrétním státu nebylo trestné - tím využije **bezpečného přístavu** daného státu - takhle může poschovávat jednotlivé činosti a vyhnout se tak stíhání - jediné řešení je mezinárodní spoluprací a to tak že se dohodnou že to budou upravovat stejně (to co je trestné u nás je trestné i u ostatních) = **harmonizace**

10.1.1 Harmonizace v TP

Společná definice toho co je a není trestný čin (definice hmotného práva trestního) tak i to jak se stíhá (definice procesního práca) - pro vydání důkazu od jiného státu je většinou potřebná dvojí trestnost (TČ v obou státech), jinak nemusí vyhovět vydání daných důkazů - pokud by se u nás stal TČ ale důkazy by byly v jiném státě, tak náš stát by popsal skutkový stav (co se stalo), jaké důkazy potřebuje a proč, pokud by to nebylo trestné i v druhém státě tak by nemohl použít jejich procesně správní prostředky a tak nemůže pomoct - proto se snaží co nejvíce harmonizovat (i procesní nástroje, aby vůbec daný důkaz mohl druhý stát zajistit)

Harmonizace je velmi složitý proces - vyždycky je tam stát, kterému se něco nelibí a tak to bojkotuje a tím se to buď vůbec nedá harmonizovat nebo to trvá strašně dlouho.

Harmonizační instrumenty (nástroje pro dosžení harmonizace):

- Mezinárodní úmluvy (smlouvy) - drívě na rozdělení vod, vesmíru a vzdušného prostoru - velmi komplikované dosáhnout společného řešení - Úmluva o kyberkriminalitě (2001 v Budapešti), původně jen Evropa ale podepsalo jí i hodně jiných států, mezinárodně nejspupěšnější
- Regionální úmluvy - platí pouze na určitém místě - lokální dohody (teritoriálně) - částečně kompatibilní - Dohoda o spolupráci při boji proti kriminalitě související s počítačovými daty (Commonwealth, 2001) - Dohoda o boji proti IT trestných činech (Arabská liga, 2010) - Dohoda o spolupráci v oblasti mezinárodní informační bezpečnosti (Shanghajská organizace spolupráce, 2010) - Úmluva o kybernetické bezpečnosti a ochraně osobních údajů (Africká unie, 2014)
- Dvoustranné úmluvy - mezi dvěma státy, bilaterární (tipicky mezi sousedními) - v kyberkriminalitě se to moc nepoužívá
- Vzorové právo - nástroj který není nijak vymahatelná, nikdo se k ničemu nezavazuje - stát v určitých regionech často nemá prostředky na vytvoření vhodné právní regulace určité oblasti - nadnárodní celky vytváří vrozové právo nebo nějaké řešení určité oblasti (problému), vpodstě říkají tady problém a my si myslíme že by se to měl řešit takhle, a vy to mužete a nemusí příjmout - státy mohou a nemusí tyto upravy příjmout - Vzorové právo pro počítačovou kriminalitu a byberkriminalitu (Jihoafrická společnost pro spolupráci) - OSN resp. UNODC se snažilo o přípravu ale připravit i vzorové právo je složité a proto jich je spoustu rozpracovaných ale nedokončených
- Právo EU - velmi specifické postavení - reguluje se regionálně - je to závazné pro všechny v daném regionu pomocí nařízení a směrnic - Směrnice o útocích na informační systémy (2013), z hlediska hmotně právní úpravy podobná Úmluvě o kyberkriminalitě

10.2 Snahy do budoucna

OSN se snaží ale jak je velká a má obrovský dopad tak je problém něco prosadit - jak má hodně členu tak se najdou ty co do toho hází vidle (čína, rusko - jim se tento stav líbí a nechtějí ho měnit, vpodstatě říkají: nepříjmeme umluvu o kyberkriminalitě protože je považujeme za lokální evropskou úmluvu, chceme vymyslet nové právo ale budem vám do toho házet vidle do té doby než se na to zapomene) - nepodařilo se příjmout ani studii o z mapování páchání kyberkriminality po světě (zůstalo to ve formě návrhu) - to se ostatním státum nelíbí a snaží se tedy co nejvíc rozšířít svojí jurisdikci (predevším EU a USA) - např GDPR (nařízeni o ochraně osobních údaju) má velmi specifickou jurisdikci, vztahuje se na všechny subjekty ať jsou usídleny kdekoliv které poskytují služby v EU (vztahuje se to i na čínu a rusko), druhá otázka je pak vymahatelnost techto pravidel - EU se to líbí a začínají to uplatňovat i do ostatních uprav - USA příjmuli CLOUD act, který říká že je jedno kde máš dat o amerických občanech, ale pokud je to v zahraničí tak má povinnost je vydat americkým úřadum (při požádáni i quess??) Do určité miri dochází k fragmentaci internetu (rusko a čína to velmi podporují) - čína si striktně dozoruje co jde dovnitř a ven z jejich internetu (velký čínský firewall), např data o čínskách občanech se nesmí uchovávat mino čínu - rusko vyhrožuje totálním odpojením jejich části sítě

10.3 Procesní právo a spolupráce

Pokud někdo nechce spolupracovat existují nástroje které se dají ohnout protřeby kyberkriminality - OČTŘ musí požádat jiný stát o spolupráci - existují ruzné mechanizmi jak se tohoto dosahuje - jeden zpusob je stát obejít a rovnou se to řeší s poskytovately konkretních služeb - obecně mívají i více lidí kteří mají ke spolupráci dostatek znalostí + vetšinou jsou to stejně oni kdo drží ty data

– formální spolupráce států - MLA (Mutual Legal Assistance) mezinárodní justiční pomoc - nejstandardnější mechanizmus upravený v mezinárodních smlouvách a ve většině právních řádů - umožňuje OČTR sepsat žádost o mezinárodní justiční spolupráci která se předá pomocí komunikujících zastupitelských úřadů a čeká se než dožádaný stát poskytně spolupráci - problém je že je to velmi pomalé (enormí birokracie) a stát na to nemusí vyhovět - jeden z požadavků je aby byla dostupné procesní nástroje v obou státech - v EU je pak další způsob -MR (Mutual Recognition) vzájemné uznávání rozhodnutí - fungující specificky v EU - na základě Evropského vyšetřovacího příkazu - uplatňuje se u některých procesních nástrojů, které upravují evropské předpisy - dožádaný stát musí příjmou (s extrémě uzkými vyjímkami) rozhodnutí jiného státu a s určitou prioritou ho musí vykonat - jsou zde lhůty(30 dní na rozhodnutí + 90 na vykonání příkazu) - odpadá část birokracia - a povynnost součinnosti - pak ještě exi-

tují Dvoustranné nástroje - dva státy se dohodnou na lepší spulupráci - většinou státy které mají k sobě blízko - většinou né v kyberkriminalitě - má me třeba se sousedníma státama že když někoho stíhají v autě a přejedou hranice tak můžou pokračovat
– Neformální spolupráce států - orgány nebo lidi se znají a tak si poskytnou spolupráci nebo se aspoň asměrují na správnou cestu/směr - konzultace, expertázy, vybavení - může to koordinovat Europol nebo Interpol nebo může být zprostředkována přes bezpečnostní týmy nebo jiné státní orgány nebo sdružení např sdružení energetických společností - neformálni cesty negenerují tak kvalitní důkazy - na druhou stranu je to o dost rychlejí - pokud třeba jen zjišťujeme kde se důkazy mohou nacházek kdo je může mít, jaký poskytovatel tak se můžeme jednoduše takhle neformálně doptat jiných států/orgánu-/společností (na tohle je to super)
– Prímá spolupráce s ISP - Existující právní regulace - Preservation and production směrnice (EU) - Cloud act (US) - nebo dobrovolná spolupráce

schéma ukazující spolupráci dvou států - zdlouhavé, vůži volatilitě el. důkazů - někdy třeba státy nevyhoví vůbec nebo třeba za 2 roky, kdy už je to jedno nástroje které definuje Úmluva o kyberkriminalitě viz. odkaz Evropský vyšetřovací příkaz - postaven na MR - vzájemné uznávání rozhodnutí - měl by přinést vetší efektivitu při mezinárodním zajišťování důkazů - nastavené lhůty (po přijetí příkazu 30 dnů na rozhodnutí jestli je nebo není proveditelný a do 90 dnu pak vykonat v případě že jde vykonat) - stejná priorita cizích rozhodnutí jako lokálních rozhodnutí - omezení kdy tomu může státat nevyhovět (protiustavní apod. hodně limitované) Přikáz k zachování a vydání data - zatím nepřijatá směrnice EU - stát by mohl vyžadovat přimo po ISP v cizí zemi vydání dat - platilo by pro ISP poskytující služby v EU - rozšiřuje to jurisdikci na všechny které poskytují služby CLOUD act - USA - americké orgány mohou přistupovat k datům spravovaných o amerických subjekterch i mimo území USA - google bude mít data o američanech uložená na serveru v EU -> má povinnost tady data vydat americkým orgánům - pro nás je zajímavá úprava executive agreements (výkonné smlouvy), které se uzavírají s určitýma regionama ve světě - jedná se o uzavření mezi US a EU, zatím neexistuje ale je snaha aby tomu tak bylo - tak by vznikla možnost vyžadování dat i opačně (po amerických poskytovatelech služeb, které by drželi udaje o češích)

10.4 Aktuální iniciativa

– UNODC - snažili se o vzorové právo, studii, která nakonec nebyla přijata - vytvořili portál kde se sdílí soudní rozhodnutí a právo ohledně kyberkriminality pro informační důvody - dále dělají vzdělávací moduly na organizovaný zločin všetně kyberkriminality (společné vzdělávání vyšetřovatelů, nebo rovojových zemí aby třeba somálsko mělo někoho kdo dokáže poskytnou spolupráci třeba) - takové měkčí iniciatiy

– Rada Evropy - tvrdší charakter než snahy UNODC - skupina odborníků která pracuje na druhém dodatkovém protokolu k Úmluvě o kyberkriminalitě - který by měl řešit problém s omezenou možností spolupráce (nové procesní nástroje pro exektivní předávání dat, videokonference, mechanismus předávání dat apod)
– EU - vytváří certifikaní mechanismus nástrojů pro vyšetřování kyberkriminality a nástroju předávání el. důkazů a pracují daných mechanismech na elektonickém předávání důkazního materiálu - neexistuje jednoznačný postup pro předání el. důkazu (někdy se převází na flashce autem, někdy nějak elektronicky - stím ale můžou mít soudy problém že to není bezpečné)

Dále pomáhají taxonomie pro kategorizaci kyberkriminality - Europská taxonomie (ENISA/EUROPOL) - společná klasifikace bezpečnostních incidentů a jejich navázání na europskou právní úpravu. Lepší statiky než kdyby se klasifikovalo na základě TP hmotného - OSN taxonomie - UNODC