NSZ ČR

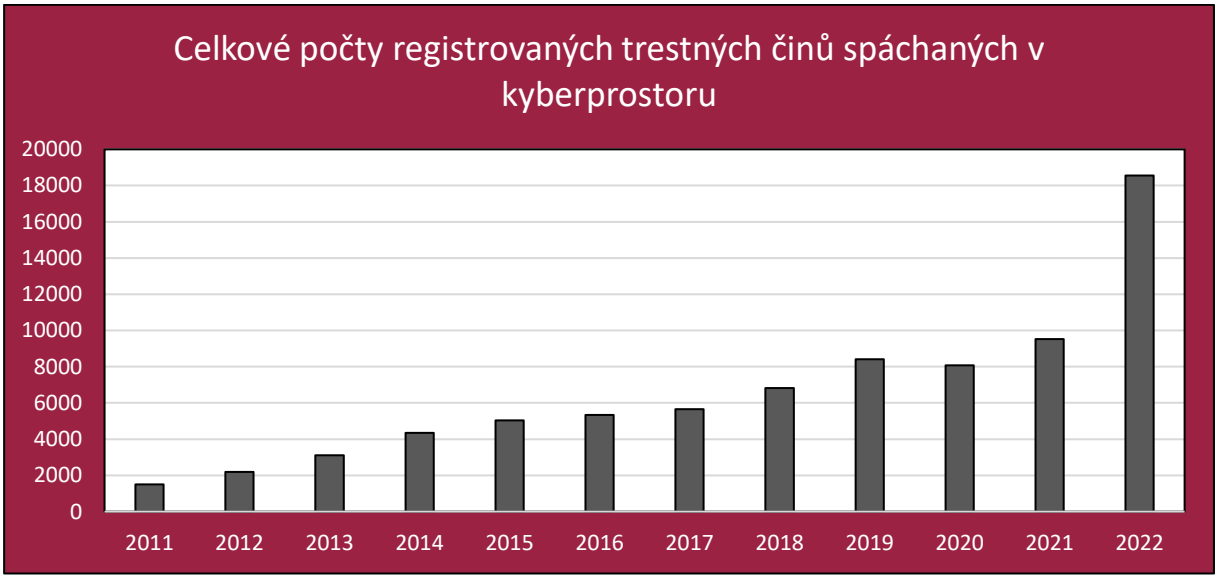
Zpráva o činnosti národního zpravodaje pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2022

Mgr. Tomáš Foldyna

V Brně dne 28. února 2023
1 SPR 101/2023

Úvodem lze v obecné rovině konstatovat, že i v roce 2022 pokračovaly v oblasti kybernetické kriminality, a zvláště v oblasti kriminality páchané v kybernetickém prostoru, trendy z předchozích let, tedy především prudký nárůst tohoto druhu kriminality. Tento vývoj je o to víc znepokojující, když oproti rokům 2020 a 2021, kdy došlo v důsledku pandemie Covid-19 k výraznému přesunu aktivit osob z reálného do virtuálního prostředí, se v r. 2022 život ve společnosti vracel postupně k normálu. Přesto však došlo téměř ke zdvojnásobení evidovaných trestných činů spadajících do této oblasti, když v loňském roce **došlo k spáchání 18 554 trestných činů v kyberprostoru oproti 9 518 trestným činům v r. 2021**.

Podíl na celkovém nápadu trestné činnosti v r. 2022 tak v případě kybernetické kriminality a kriminality páchané v kybernetickém prostoru překonal 10 %.



Pokračoval dřívější dynamický rozvoj informačních technologií a jejich uvádění na trh v neustálých vylepšeních a obměnách (koncové šifrování komunikace je standardem, stejně jako využití biometrických dat, bezdrátové šifrované přenosy mezi synchronizovanými zařízeními, masivní ukládání dat ve vzdálených úložištích, stále se zjednodušující možnosti využití kryptoměn, moderní elektronické platební metody atd.).

S tím vším pochopitelně souvisel také nárůst a další přesun páchání trestné činnosti z reálného prostoru do kyberprostoru. Přesto je však překvapující, že celkový nápad tohoto druhu trestné činnosti vzrostl prakticky o 100 %, přičemž navíc lze důvodně předpokládat, že část skutečně spáchaných trestných činů zůstává ze strany poškozených neohlášena, např. z důvodu, že poškozeným nevznikla škoda majetkového charakteru.

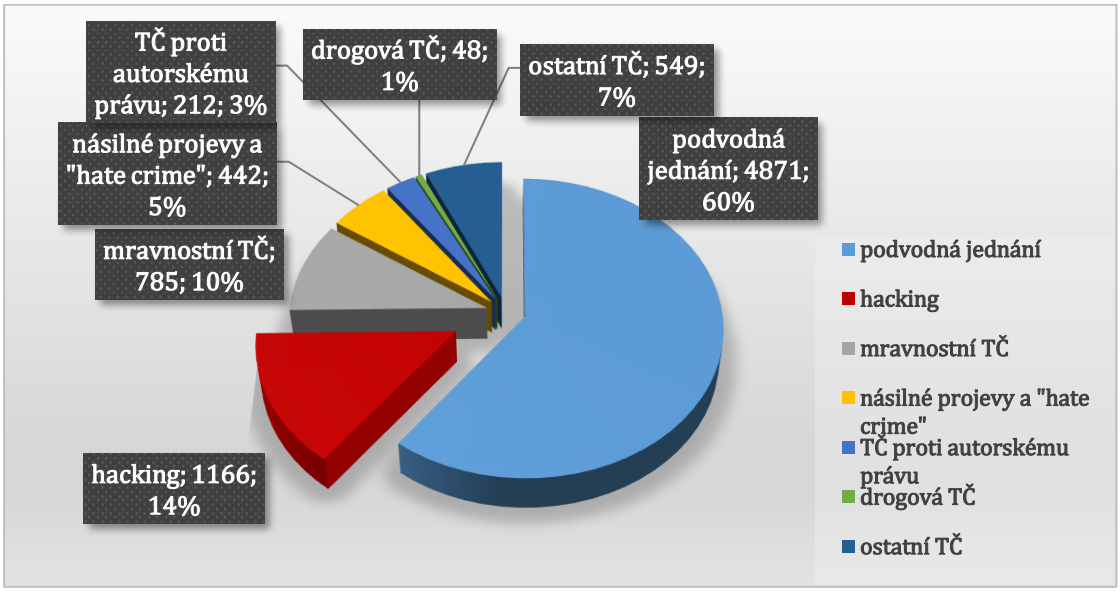
Z mezinárodních informací a zkušeností také vyplývá, že v průběhu r. 2022 pokračoval trend porušování autorských práv na internetu, jako např. streamování filmů, hudby a počítačových her. Tato trestná činnost však zůstává vysoce latentní a velmi těžko odhalitelná a dokladovatelná, takže se neprojevuje v oficiálních statistikách kybernetické kriminality, resp. kriminality páchané v kyberprostoru.

Události a trendy v oblasti kyberkriminality v roce 2022

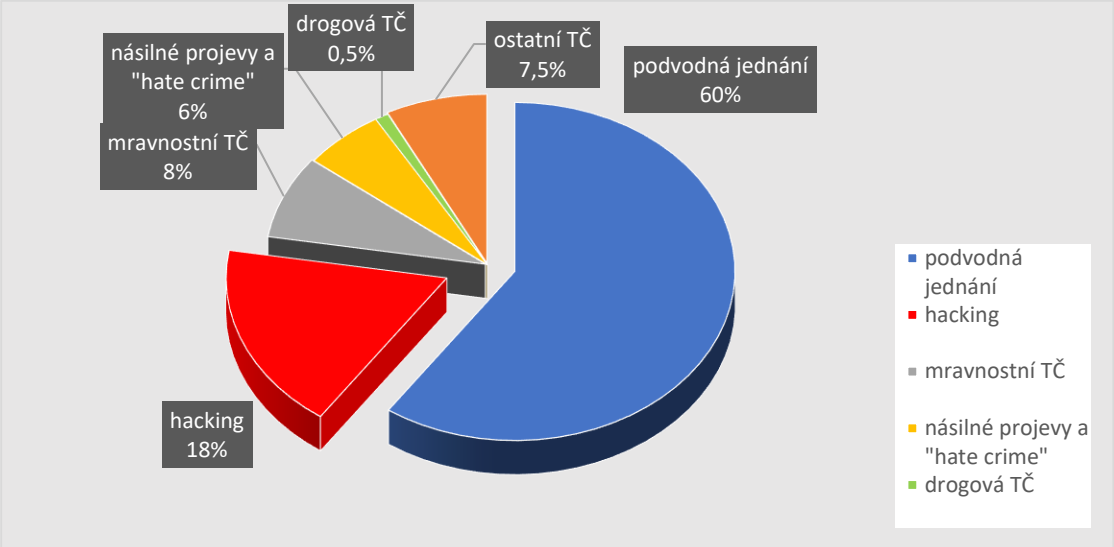
Jak už je výše uvedeno, došlo v r. 2022 ke zvýšení celkové kriminality spáchané v kyberprostoru (kyberkriminalita v širším i v užším slova smyslu) o 94,9 %, což je alarmující fakt, na který reaguje jak Policie ČR, tak státní zastupitelství posilováním svých kapacit na tomto úseku kriminality (viz níže).

Následující grafy převzaté z údajů Policie ČR znázorňují skladbu trestné činnosti páchané v kyberprostoru v letech 2021 a 2022.

R. 2021



R. 2022



Jak je patrno z výše uvedených grafů, tak skladba trestné činnosti v kybernetickém prostoru se meziročně nijak výrazněji nezměnila, takže ve všech dílčích úsecích došlo k prakticky stejnému zvýšení nápadu, což znamená téměř zdvojnásobení ve všech směrech.

Výrazně medializována však v loňském roce byla problematika majetkové trestné činnosti páchané prostřednictvím internetu. Nadále pokračovaly podvody typu „americký voják hledá přítelkyni v ČR“, kdy pachatel po navázání bližšího kontaktu a získání důvěry oběti (zpravidla ženy) začne po oběti žádat zasílání dalších a dalších finančních prostředků pod záminkou přestěhování věcí a převodu svých finančních prostředků do ČR, aby mohl za obětí přicestovat a žít s ní.

Druhým typem internetových podvodů, který v loňském roce zaznamenal prudký růst, je podvodná nabídka „výhodného“ obchodování s kryptoměnami, kdy pod záminkou nákupu kryptoměny jsou z oběti vylákány značné finanční prostředky.

Velmi časté jsou také podvodné reakce na inzertní nabídky prodeje zboží, kdy pachatel kontaktuje prodávajícího s nabídkou, že zboží uhradí převodem na účet prodávajícího a zboží poté odveze zásilková služba. Za tímto účelem se pak snaží pachatel vylákat z poškozeného přístupové údaje k jeho platební kartě, kterou následně zneužije a odčerpá finanční prostředky z účtu poškozeného.

A nakonec, velmi se v r. 2022 rozšířily podvody založené na sociálním inženýrství, jejichž podstatou je snaha dostat oběť pod tlak, často pomocí fingovaných telefonátů „bankéře“ upozorňujícího na probíhající „útok“ na účet oběti, která je pak pod hrozbou tohoto nebezpečí přinucena, resp. přesvědčena ke sdělení svých přístupových údajů k účtu nebo k platebním prostředkům (platebním kartám) a následně pak dojde k odcizení veškerých finančních prostředků z účtu oběti.

Nadále také pokračovaly již „běžné“ formy podvodného jednání na internetu jako phishing či získávání přístupu k platebním kartám pod záminkou objednání a koupě

zboží.

Strmý nárůst zaznamenala v r. 2022 také kyberkriminalita v užším slova smyslu, tzv. „hacking“ (zejména § 230 trestního zákoníku). Zde se jedná zejména o útoky na soukromé účty osob na sociálních sítích s cílem následného vydírání nebo navazujícího podvodného jednání.

Naproti tomu v r. 2022 nerostl počet ransomwarových útoků a zejména již nedocházelo k tak masivním ransomwarovým útokům jako v dřívějších letech.

Nadále platí v rámci ČR i v rámci celé Evropy, že kybernetické kriminalitě a kriminalitě v kybernetickém prostoru nahrává nízké právní i technické vědomí veřejnosti v kombinaci s poměrně omezenými schopnostmi rozpoznat, předcházet a bránit se útokům využívajícím informační technologie, stejně jako nedostatečná regulace, která se jak na národní, tak na celoevropské úrovni značně zpožďuje za dynamickým rozvojem informačních technologií. Zatímco šifrování, využívání kryptoměn, používání biometrie k ověřování přístupů a transakcí je již dnes standardem, stejně jako ukládání dat ve vzdálených úložištích, právní rámce jednotlivých zemí i EU jako celku si neví rady, jak tuto problematiku regulovat, takže orgány činné v trestním řízení narážejí na limity spočívající v nemožnosti opatření některých dat (elektronických důkazů) pro účely trestního řízení, neboť nemají právní nástroje, jak tyto data získat. Problémy při nastavení právního rámce regulace této oblasti jsou dány především konfliktem mezi potřebami orgánů činných v trestním řízení pronikat do soukromí uživatelů při objasňování těchto forem trestné činnosti a mírou zajištění ochrany základních práv a svobod těchto uživatelů, zvláště pak mírou ochrany jejich soukromí při užívání informačních technologií.

Stále více a více se tak ukazuje být problematickým současný nedostatečný právní rámec, který neukládá poskytovatelům povinnost registrovat údaje o využití služeb VPN, šifrování atd., což vede k tomu, že řada pachatelů závažných trestných činů zůstává skryta v anonymním prostředí internetu nebo darknetu.

Významná judikatura

Z hlediska opatřování elektronických důkazů je nutno zmínit další z řady rozhodnutí Soudního dvora EU zabývající se problematikou uchovávání provozních a lokalizačních údajů (data retention), konkrétně **rozhodnutí ve spojených věcech C-793/19 SpaceNet a C-794/19 Telekom Deutschland, ze dne 20. září 2022, v němž**
Soudní dvůr EU potvrdil svou dřívější judikaturu vystavěnou na právním názoru, že unijní právo brání plošnému a nerozlišujícímu uchovávání provozních a lokalizačních údajů s výjimkou případů vážného ohrožení veřejné bezpečnosti. Za účelem boje proti závažné trestné činnosti však mohou členské státy při striktním dodržování zásady proporcionality stanovit zejména cílené nebo urychlené uchovávání takových údajů, jakož i plošné a nerozlišující uchovávání IP adres.

Meritum věci:

Společnosti SpaceNet a Telekom Deutschland poskytují v Německu veřejně dostupné služby internetového připojení. Před německými soudy tyto společnosti napadly povinnost uchovávat od 1. července 2017 telekomunikační provozní a lokalizační údaje svých zákazníků, kterou jim ukládá německý zákon o telekomunikacích (TKG). TKG ukládá poskytovatelům výše zmíněných služeb zejména za účelem stíhání závažných trestných činů nebo odvrácení konkrétního nebezpečí pro národní bezpečnost, plošné a nerozlišující uchovávání zásadních provozních a lokalizačních údajů koncových uživatelů po dobu několika týdnů. Německý Spolkový správní soud požádal SDEU o vyjasnění, zda unijní právo brání takové vnitrostátní právní úpravě. Jeho pochybnosti vyplývají zejména ze skutečnosti, že povinnost uchovávat údaje stanovená TKG se týká nižšího počtu údajů a kratší doby uchovávání (4 nebo 10 týdnů), než stanoví vnitrostátní právní předpisy dotčené ve věcech, v nichž byly vydány předchozí rozsudky. Tyto zvláštnosti omezují možnost, že by uchovávané údaje umožnily vyvodit velmi přesné závěry o soukromém životě osob, jejichž údaje byly uchovávány.

Rozhodnutí

Soudní dvůr v rozsudku potvrdil svou judikaturu a stanovil, že unijní právo **brání** vnitrostátní právní úpravě, která pro účely boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti preventivně stanoví plošné a nerozlišující uchovávání provozních a lokalizačních údajů.

Naproti tomu unijní právo **nebrání** vnitrostátní právní úpravě:

- *která za účelem zajištění národní bezpečnosti stanoví možnost přikázat poskytovatelům služeb elektronických komunikací, aby prováděli plošné a nerozlišující uchovávání provozních a lokalizačních údajů v situacích, kdy dotyčný členský stát čelí závažnému ohrožení národní bezpečnosti, které se jeví jako skutečné a aktuální nebo předvídatelné. Takový příkaz může být přezkoumán buď soudem, nebo nezávislým správním orgánem a může být vydán pouze na dobu nezbytně nutnou, avšak s možností prodloužení, pokud toto ohrožení přetrvává;*
- *která za účelem zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti stanoví cílené uchovávání provozních a lokalizačních údajů,*
- *které je na základě objektivních a nediskriminačních kritérií vymezeno kategoriemi dotčených osob nebo prostřednictvím zeměpisného kritéria, na dobu nezbytně nutnou, avšak s možností prodloužení;*
- *která za stejnými účely stanoví **plošné a nerozlišující uchovávání IP adres** přidělených zdroji připojení, a to po nezbytně nutnou dobu;*
- *která za účelem zajištění národní bezpečnosti, boje proti trestné činnosti a veřejné bezpečnosti stanoví plošné a nerozlišující uchovávání údajů o totožnosti uživatelů prostředků elektronické komunikace;*

- *která za účelem boje proti závažné trestné činnosti a a fortiori zajištění národní bezpečnosti stanoví možnost přikázat poskytovatelům služeb elektronických komunikací, aby po určenou dobu prováděli urychlené uchování provozních a lokalizačních údajů, jimiž tito poskytovatelé služeb disponují.*

Taková vnitrostátní právní úprava kromě toho musí pomocí jasných a přesných pravidel zajistit při uchovávání dotčených údajů dodržení souvisejících hmotněprávních a procesních podmínek, a to že subjekty údajů mají k dispozici účinné záruky proti riziku zneužití.

Povinnost uchovávání stanovená TKG se vztahuje na velmi široký soubor provozních a lokalizačních údajů. Tento soubor provozních údajů uchovávaných po dobu deseti týdnů a lokalizačních údajů uchovávaných po dobu čtyř týdnů přitom umožňuje vyvodit přesné závěry o soukromém životě osob, jejichž údaje jsou uchovávány. Pokud jde o záruky stanovené TKG, jejichž cílem je chránit uchovávané údaje před riziky zneužití a před jakýmkoli protiprávním přístupem, Soudní dvůr uvádí, že uchovávání těchto údajů a přístup k nim představují samostatné zásahy do základních práv subjektů údajů vyžadující samostatné odůvodnění. Z toho vyplývá, že vnitrostátní právní předpisy zajišťující plné dodržování podmínek vyplývajících z judikatury v oblasti přístupu k uchovávaným údajům nemohou být z povahy věci způsobilé omezit, či dokonce zhojit závažný zásah do práv subjektů údajů, který by vyplýval z plošného uchovávání těchto údajů.

Plné znění rozsudku v češtině je k dispozici zde.

V souvislosti s problematikou „data retention“ pak stojí za připomenutí rozhodnutí Nejvyššího soudu ze dne 21. dubna 2022, sp. zn. 6 Tdo 266/2022, kdy právě v této projednávané trestní věci, stejně jako v řadě jiných, byly provozní a lokalizačních údaje využity k usvědčení pachatelů.

Z odůvodnění:

*„Důvodnými pak nejsou ani námitky zpochybňující závěry o konání schůzky dne 30. října 2015. Obvinění ve své argumentaci zúžili tuto problematiku na hodnocení poznatků získaných z **buněk BTS**, přičemž zdůrazňovali (mimo jiné poukazem na znalecký posudek), že **z nich nelze jednoznačná zjištění činit**. Z odůvodnění napadených rozhodnutí ovšem vyplývá, že soud prvního stupně tyto poznatky nehodnotil jako stěžejní důkaz, ale interpretoval je **jednak jako vyvrácení tvrzení obviněného F.**, že se v inkriminované době nacházel na hřbitově v obci XY, tedy mimo XY, a jednak jako **potvrzení dalších nepřímých důkazů**, když ze záznamů buněk BTS je patrný pohyb telefonů obou obviněných do stejné lokality v rámci XY. Žádné přesnější závěry k jejich lokalizaci z tohoto důkazu nečinil, ale vycházel z **komplexního hodnocení celého provedeného dokazování**. Odvolací soud potom v odstavci 7. svého usnesení pouze konstatoval, že mobilní telefony se pohybovaly v určité době v určitém společném okruhu, přičemž jejich přesnou polohu zaměřit nelze. Fakticky tedy obvinění tomuto jednotlivému důkazu, který nebyl způsobilý podat přesné údaje o jejich lokalizaci, přikládají přílišný význam, a to v rozporu s hodnotícími závěry soudů. Ty dovozovaly svá skutková zjištění z širokého okruhu provedených*

důkazů, zejména z obsahu telefonické komunikace obviněných a následné reakce obviněného R. na zjištěné informace jak v kontaktu se svědkem Ch., se kterým své nabyté poznatky sdílel, tak i v jeho „podnikatelské“ aktivitě, na níž byla zaměřena pozornost orgánů PČR. Pohyb mobilních telefonů obviněných přitom hodnotily jako nepřímé potvrzení takto činěných závěrů.“

Z pohledu státního zastupitelství lze za další významné rozhodnutí v oblasti kybernetické kriminality považovat **usnesení Nejvyššího soudu ze dne 30. srpna 2022, sp. zn. 4 Tdo 376/2022,** řešící problematiku totožnosti skutku v případě trestného činu podle § 230 trestního zákoníku.

Legislativa

V průběhu r. 2022 nadále pokračovaly rekodifikační práce na novém trestním řádu, který by měl znamenat pokrok v oblasti opatřování a zajišťování elektronických důkazů, ať už v rámci právní úpravy operativně pátracích prostředků nebo zajišťovacích institutů. Tyto práce jsou nyní ve fázi kompletace celého nového trestního řádu a jeho připomínkování ze strany odborné veřejnosti.

Dnem 6. srpna 2022 své účinnosti nabyl **zákon č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**, ve znění pozdějších předpisů. Účelem novely je zajištění adaptace českého právního řádu na evropské nařízení 2019/881 o agentuře ENISA (Agentura Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií. Vnitrostátním orgánem certifikace kybernetické bezpečnosti stanovuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a dále doplňuje možnosti správního trestání za porušení povinností ze zákona vyplývajících.

Na celoevropské úrovni došlo k přijetí následující legislativy:

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2.0)

Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (směrnice CER)

Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (nařízení DORA)

Uvedené právní předpisy EU se však spíše týkají zajištění kybernetické bezpečnosti než kybernetické kriminality v užším slova smyslu.

Nadále také pokračovaly legislativní práce na evropské úrovni týkající se zejména plánovaného nařízení o soukromí a elektronických komunikacích (ePrivacy nařízení), které by do budoucna mohlo dát vzniku nové právní úpravě data retention.

Rovněž tak pokračovala vyjednávání na půdě OSN ohledně zcela nové úmluvy proti kybernetické kriminalitě, které však nijak výrazně nepokročily v důsledku pandemie onemocnění Covid-19.

Vnitrostátní aktivity na úseku kybernetické kriminality

Na počátku r. 2022 schválil nejvyšší státní zástupce celkovou koncepci rozvoje schopností státního zastupitelství na úseku boje proti kybernetické kriminalitě a kriminalitě v kybernetickém prostoru.

V návaznosti na schválení této koncepce došlo k novelizaci pokynu obecné povahy nejvyššího státního zástupce č. 4/2009, Vzorového organizačního řádu, a došlo s účinností k 1. lednu 2023 k vyčlenění zcela samostatné specializace státních zástupců pod označením „Kybernetická trestná činnost a trestná činnost v kybernetickém prostoru“. Specializovaní státní zástupci by se měli v budoucnu přednostně zaměřovat na dozor nad zachováváním zákonnosti v přípravném řízení ve věcech naplňujících definiční kritéria tohoto druhu kriminality.

Nejzávažnějším případům kybernetické kriminality spočívajícím v útocích na kritickou informační infrastrukturu státu by se pak v nejbližší době měli začít věnovat státní zástupci vrchních státních zastupitelství (Praha a Olomouc). Nejvyšší státní zastupitelství již v tomto směru navrhlo Ministerstvu spravedlnosti ČR příslušnou novelu jednacího řádu státního zastupitelství (vyhláška č. 23/1994 Sb.).

Po ukončení protipandemických opatření došlo v r. 2022 rovněž k znovuobnovení činnosti sítě specialistů státního zastupitelství v oblasti kybernetické kriminality, která je tvořena specializovanými státními zástupci ze všech organizačních článků státního zastupitelství. Celkově se tato síť specialistů v uplynulém roce sešla dvakrát, aby si jednak předala informace o nových trendech v dané oblasti a seznámila se s novými postupy Policie ČR při objasňování tohoto druhu kriminality, jakož i s přípravami vzniku nové policejní centrály zaměřené na boj proti kyberkriminalitě (Národní centrála proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování; vznik 1. ledna 2023), a jednak vypracovala vstupní kritéria pro přípravu nové koncepce vzdělávání státních zástupců specializovaných na problematiku kybernetické kriminality.

Tato nová koncepce vzdělávání je rovněž připravována na základě rozhodnutí nejvyššího státního zástupce a vyplývá z koncepce rozvoje schopností státního zastupitelství na daném úseku. Cílem je vytvoření uceleného programu vzdělávání, v jehož rámci by státní zástupci získali veškeré informace a vědomosti o kybernetické trestné činnosti a o trestné činnosti páchané v kybernetickém prostoru, o technické

stránce tohoto druhu kriminality i o souvisejících právních aspektech vyplývajících z právní úpravy i aktuální judikatury.

Již nyní se však státní zástupci coby lektoři aktivně podílejí na organizaci vzdělávacích akcí na téma kyberkriminality pořádaných Justiční akademií ČR.

Za významnou rovněž považujeme soustavnou a úzkou spolupráci státního zastupitelství a Národního úřadu pro kybernetickou a informační bezpečnost, a to jak v rovině konzultací, tak v rovině účasti na vzdělávacích nebo popularizačních akcích pro odbornou, ale i laickou veřejnost.

Zahraniční aktivity na úseku kybernetické kriminality

Státní zastupitelství se spolu s Ministerstvem spravedlnosti ČR a Policií ČR v uplynulém roce výrazně podílelo na zajištění rozvojové spolupráce organizované Ministerstvem zahraničních věcí, když státní zástupci spolu s dalšími specialisty předávali zkušenosti z boje proti kybernetické kriminalitě svým kolegům z Bosny a Hercegoviny, Ghany a Senegalu.

Státní zástupci se rovněž účastní dalších aktivit na mezinárodní úrovni, z nichž mezi nejvýznamnější v současné době patří vyjednávání zcela nové úmluvy proti kybernetické kriminalitě na půdě OSN.

Další významnou nadnárodní aktivitou, na níž se státní zástupci podílejí, je činnost Evropské sítě proti kybernetické kriminalitě, která funguje v rámci Eurojustu a která přispívá ke sdílení zkušeností z boje proti tomuto druhu kriminality nejen mezi jednotlivými státy EU, ale také mezi dalšími přidruženými státy.

Hlavní výzvy pro r. 2023

1) Za hlavní výzvu v roce 2023 považuji zlepšování stávajícího nedostatečného právního rámce pro boj s kyberkriminalitou.

2) S ohledem na setrvalý růst trestné činnosti páchané v kyberprostoru se jeví jako nutné urychleně rozvíjet síť specialistů a dokončit a realizovat systém jejich komplexního vzdělávání.

3) Udržení a další rozvoj aktivit na mezinárodní úrovni, které výrazně ovlivňují pozici ČR při vyjednávání o nadnárodních instrumentech boje proti kybernetické kriminalitě.

4) Posílení lidských zdrojů v oblasti boje proti kybernetické kriminalitě.

Závěrem je potřeba také upozornit, že v r. 2022 narůstal počet incidentů, které se jeví jako útoky, za nimiž stojí cizí státní moc. To samozřejmě souvisí i s probíhající válkou na Ukrajině a postojem ČR k ní.

Z výše uvedeného je zřejmé, že obraně před kybernetickými útoky jak jednotlivců, tak i státních aktérů je nutno do budoucna věnovat stále větší pozornost a investovat jak do materiálového vybavení, tak hlavně do lidských zdrojů, které by měly tomuto narůstajícímu nebezpečí čelit. Stejně tak je nutno zaměřit pozornost na vybudování moderního právního rámce, který umožní účinně se s těmito riziky vypořádat za současného zajištění ochrany základních práv a svobod v míře obvyklé v demokratickém právním státě.