



Rada
Evropské unie

Brusel 17. května 2021
(OR. en)

8640/21

LIMITE

CYBER 138
JAI 523
DATAPROTECT 125
TELECOM 194
MI 332
CSC 190
CSCI 78

Interinstitucionální spis:
2020/0359(COD)

POZNÁMKA

Odesílatel:	Předsednictví
Příjemce:	Výbor stálých zástupců / Rada
Předmět:	Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 – zpráva o pokroku

Za vypracování této zprávy odpovídá předsednictví a nejsou jí dotčeny konkrétní body zájmu ani další příspěvky jednotlivých členských států. Zpráva popisuje práci, která byla dosud vykonána v přípravných orgánech Rady, a současný stav posuzování výše uvedeného návrhu. Rada se vyzývá, aby vzala tuto zprávu na vědomí.

I. ÚVOD

1. Dne 16. prosince 2020 přijala Komise návrh směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii („revidovaná směrnice o bezpečnosti sítí a informací“ nebo „směrnice NIS 2“)¹, jehož účelem bylo nahradit stávající směrnici o bezpečnosti sítí a informačních systémů („směrnice o bezpečnosti sítí a informací“)². Návrh byl jedním z opatření plánovaných ve strategii kybernetické bezpečnosti EU pro digitální dekádu³, jejichž cílem je vybudovat odolnost vůči kybernetickým hrozbám a zajistit, aby občané a podniky těžili z důvěryhodných digitálních technologií.
2. Cílem návrhu, založeného na článku 114 SFEU, je dále zlepšit odolnost veřejných a soukromých subjektů, příslušných orgánů a Unie jako celku i jejich schopnosti reagovat na bezpečnostní incidenty. Návrh významně rozšiřuje oblast působnosti stávající směrnice o bezpečnosti sítí a informací, zabývá se bezpečností dodavatelských řetězců, posiluje ukládané bezpečnostní požadavky, zjednodušuje oznamovací povinnosti a zároveň zavádí přísnější dohledová opatření i vymáhání. Rovněž obsahuje ustanovení zabývající se sdílením informací a spoluprací v oblasti řízení kybernetických krizí na vnitrostátní a unijní úrovni. Návrh dále upravuje regulaci databází údajů o registraci domén.

¹ Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148, COM(2020)823 final.

² Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

³ Dokument 14133/20.

3. V Evropském parlamentu je příslušným výborem pro návrh Výbor pro průmysl, výzkum a energetiku (ITRE), přičemž výbory vydávajícími stanovisko jsou Výbor pro zahraniční věci (AFET), Výbor pro vnitřní trh a ochranu spotřebitelů (IMCO), Výbor pro dopravu a cestovní ruch (TRAN) a Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE). Zpravodajem pro tento návrh je Bart Groothuis (Renew, Nizozemsko). Portugalské předsednictví uspořádalo dne 29. ledna 2021 neformální výměnu názorů na tento návrh se zpravodajem výboru ITRE. Dne 12. dubna 2021 předsednictví jednalo se zástupcem zpravodajů, Mortenem Lokkegaardem (Renew, Dánsko) z výboru IMCO. Dne 16. dubna uspořádalo portugalské předsednictví neformální výměnu názorů na tento návrh s vedoucím oddělení a dalšími administrativními pracovníky výboru ITRE. Zpravodaj představil svůj návrh zprávy ve výboru ITRE dne 3. května 2021⁴.
4. Evropský hospodářský a sociální výbor přijal stanovisko dne 28. dubna 2021⁵.
5. Dne 3. února 2021 se Výbor stálých zástupců rozhodl návrh konzultovat s Evropským výborem regionů⁶. Evropský výbor regionů své stanovisko dosud nevydal.
6. Evropský inspektor ochrany údajů přijal stanovisko dne 11. března 2021⁷.
7. V prohlášení⁸ ze dne 26. února 2021 vyzvala Evropská rada spolunormotvůrce, aby urychleně pokročili v práci, zejména pokud jde o revidovanou směrnici o bezpečnosti sítí a informačních systémů (směrnice NIS 2).

⁴ Dokument 2020/0359(COD).

⁵ Dokument TEN/730-EESC-2020.

⁶ Dokument 5573/21.

⁷ Stanovisko 5/2021 ke strategii kybernetické bezpečnosti EU a směrnici NIS 2.

⁸ <https://www.consilium.europa.eu/cs/press/press-releases/2021/02/26/statement-of-the-members-of-the-european-council-25-26-february-2021/>

8. V závěrech⁹ ze dne 22. března 2021 týkajících se strategie kybernetické bezpečnosti EU pro digitální dekádu Rada uznala, jak je důležité uplatňovat ve vztahu ke kybernetické bezpečnosti v Unii komplexní a horizontální přístup za plného respektování pravomocí a potřeb členských států, jakož i neustále podporovat technickou pomoc a spolupráci při budování kapacit členských států. S ohledem na vývoj kybernetických hrozeb vzala Rada na vědomí nový návrh směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v celé Unii, jenž vychází ze směrnice o bezpečnosti sítí a informací, a znovu potvrdila, že podporuje posilování a harmonizaci vnitrostátních rámců kybernetické bezpečnosti a trvalé spolupráce mezi členskými státy. Dále zdůraznila potřebu sladit a formulovat odvětvové právní předpisy v této oblasti.

II. ČINNOST V RÁMCI PŘÍPRAVNÝCH ORGÁNŮ RADY

9. V Radě návrh posuzuje Horizontální pracovní skupina pro otázky týkající se kybernetiky. Na neformální videokonferenci Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 17. prosince 2020 představila Komise novou strategii kybernetické bezpečnosti a návrh na přezkum směrnice o bezpečnosti sítí a informací. Následně Komise dne 12. ledna 2021 uskutečnila detailnější prezentaci návrhu.
10. Během neformální videokonference Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 19. ledna 2021 nastínilo portugalské předsednictví svou metodiku práce, pokud jde o jednání o revidované směrnici o bezpečnosti sítí a informací. Předsednictví předpokládalo důkladné čtení návrhu, přičemž vzalo v úvahu důležité novinky obsažené v revidované směrnici a umožnilo delegacím, aby se vyjádřily a předložily písemné otázky, k nimž Komise následně podala vysvětlení.

⁹ Dokument 6722/21.

11. Horizontální pracovní skupina pro otázky týkající se kybernetiky dále projednala interakci revidované směrnice o bezpečnosti sítí a informací s odvětvovými právními předpisy, zejména se směrnicí o odolnosti kritických subjektů (směrnice CER) a nařízením o digitální provozní odolnosti finančního sektoru (nařízení DORA). Komise (GŘ pro migraci a vnitřní věci) předložila nový návrh směrnice CER, v němž zdůraznila hlavní prvky interakce s revidovanou směrnicí o bezpečnosti sítí a informací. Na svých zasedáních se Horizontální pracovní skupina pro otázky týkající se kybernetiky rovněž zabývala vazbami na navrhované nařízení o digitální provozní odolnosti finančního sektoru, a to prostřednictvím poznámky k diskusi předložené předsednictvím Pracovní skupiny pro finanční služby (jež odpovídá za jednání o nařízení DORA) a také na základě prezentace pracovního dokumentu, který se zabývá vztahem mezi orgány odpovědnými za bezpečnost sítí a informací a příslušným vnitrostátním orgánem podle nařízení DORA a jež v rámci Pracovní skupiny pro finanční služby předložily tři členské státy. Předseda Horizontální pracovní skupiny pro otázky týkající se kybernetiky se rovněž zúčastnil zasedání Pracovní skupiny pro civilní ochranu, aby představil aktuální stav jednání o revidované směrnicí o bezpečnosti sítí a informací. Předsednictví pravidelně informovalo Horizontální pracovní skupinu pro otázky týkající se kybernetiky o vývoji příslušných jednání o daných návrzích, jež probíhala v rámci Pracovní skupiny pro civilní ochranu a Pracovní skupiny pro finanční služby, a znovu v souvislosti s těmito návrhy zdůraznilo potřebu úzké spolupráce na vnitrostátní úrovni mezi jednotlivými příslušnými ministerstvy.
12. Na neformálních videokonferencích konaných ve dnech 2. a 9. února 2021 zahájila Horizontální pracovní skupina pro otázky týkající se kybernetiky přezkum prvních dvou článků návrhu („Předmět“ a „Oblast působnosti“), jakož i příloh I a II. Během svého zasedání dne 2. února si Horizontální pracovní skupina pro otázky týkající se kybernetiky vyslechla prezentaci Komise a předsedy skupiny pro spolupráci v oblasti bezpečnosti sítí a informací týkající se aktuálního stavu práce v této skupině, včetně její úlohy při usnadňování provádění směrnice o bezpečnosti sítí a informací. Na výše uvedeném zasedání rovněž přednesl prezentaci výkonný ředitel Agentury Evropské unie pro kybernetickou bezpečnost (ENISA), v níž představil pracovní program této agentury, včetně informací týkajících se studie o investicích do bezpečnosti sítí a informací, kterou agentura ENISA provedla, a její úlohu při podpoře členských států a orgánů EU při provádění politiky a poradenství v souvislosti se směrnicí o bezpečnosti sítí a informací. Během těchto setkání proběhla věcná jednání ohledně oblasti působnosti a byly vzneseny otázky týkající se proporcionality.

13. Na zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 22. února 2021 předložila Komise posouzení dopadů pro přezkum směrnice o bezpečnosti sítí a informací a pokračovalo se v diskuzích o návrhu, konkrétně o člancích 3 a 4 („Minimální harmonizace“ a „Definice“).
14. Předběžné posouzení návrhu pokračovalo na zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 2. března 2021 rozsáhlými diskuzemi o člancích 5 a 6 („Národní strategie kybernetické bezpečnosti“ a „Koordinované zveřejňování informací o zranitelnostech a Evropský registr zranitelností“), přičemž Komise přednesla k problematice koordinovaného zveřejňování informací o zranitelnostech a Evropskému registru zranitelností obsáhlou prezentaci.
15. Na zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 9. března 2021 se pokračující diskuze zaměřily na články 7 až 11, které se týkají vnitrostátních rámců pro řešení kybernetických bezpečnostních krizí, příslušných vnitrostátních orgánů a jednotných kontaktních míst podle revidované směrnice o bezpečnosti sítí a informací a bezpečnostních týmů typu CSIRT („týmy CSIRT“), včetně jejich požadavků, úkolů a spolupráce na vnitrostátní úrovni.
16. Na svém mimořádném zasedání dne 17. března 2021 projednala Horizontální pracovní skupina pro otázky týkající se kybernetiky články 12 až 16 (kapitola III „Spolupráce“), které zahrnují skupinu pro spolupráci v oblasti bezpečnosti sítí a informací, síť CSIRT, evropskou síť styčných organizací pro kybernetické krize (EU-CyCLONe), zprávu o stavu kybernetické bezpečnosti v Unii a problematiku vzájemných hodnocení. Zejména v souvislosti s těmito články byla položena a objasněna řada otázek. Vedoucí týmu pro prevenci a rehabilitaci působícího v Evropském centru pro boj proti kyberkriminalitě (E3) v rámci Europolu přednesl na tomto zasedání prezentaci, která se zaměřovala na postoj donucovacích orgánů k revidované směrnici o bezpečnosti sítí a informací, a rovněž byl projednán článek 17 „Správa a řízení“.
17. Na zasedání konaném dne 24. března 2021 se Horizontální pracovní skupina pro otázky týkající se kybernetiky zabývala kapitolou IV „Řízení kybernetických bezpečnostních rizik a oznamovací povinnosti“, konkrétně článkem 18 („Opatření k řízení rizik v oblasti kybernetické bezpečnosti“), článkem 19 („Koordinované posouzení rizik kritických dodavatelských řetězců v EU“) a článkem 20 („Oznamovací povinnosti“), přičemž tento poslední článek je považován za jedno z hlavních ustanovení revidované směrnice o bezpečnosti sítí a informací.

18. Na zasedání dne 14. dubna se Horizontální pracovní skupina pro otázky týkající se kybernetiky zabývala článkem 21 („Použití evropských systémů certifikace kybernetické bezpečnosti“), článkem 22 („Standardizace“) a článkem 23 („Databáze doménových jmen a registračních údajů“), jakož i následujícími články 24 a 25 („Pravomoc a registrace“). Na tomto zasedání byla rovněž projednány kapitola V (týkající se sdílení informací) a kapitola VI (zabývající se dohledem a vymáháním). Článek 29 „Dohled a vymáhání u základních subjektů“ a článek 30 „Dohled a vymáhání u důležitých subjektů“ vyvolaly ze strany členských států řadu připomínek a otázek kvůli své obsáhlosti a podrobnosti. Rovněž byly vneseny podstatné připomínky a dotazy k článkům 31, 32 a 33, které se týkají správních pokut, porušení povinností spočívajících v porušení zabezpečení osobních údajů a sankcí. Členské státy rovněž požádaly o další objasnění týkající se článku 34 o vzájemné pomoci.
19. Na zasedání dne 19. dubna se Horizontální pracovní skupina pro otázky týkající se kybernetiky zabývala kapitolou VII „Přechodná a závěrečná ustanovení“ (články 35 až 43), čímž bylo čtení článků dokončeno.
20. Kompletní čtení návrhu bylo uzavřeno diskuzí o odůvodnění, která se uskutečnila na zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 28. dubna 2021. Jednalo se o první fyzické zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky věnované revidované směrnici o bezpečnosti sítí a informací, které se konalo během portugalského předsednictví. Srovnávací tabulku obsahující body odůvodnění a příslušné články znění předložila Komise již dne 15. února 2021.
21. Na zasedání konaném dne 5. května 2021 uspořádala Horizontální pracovní skupina pro otázky týkající se kybernetiky první výměnu názorů s cílem zahájit vypracovávání uvedeného návrhu. Aby se v této souvislosti dosáhlo pokroku, předsednictví se rozhodlo, že proces přípravy návrhu bude zahájen vypracováním otázky interakce revidované směrnice o bezpečnosti sítí a informací s příslušnými odvětvovými právními předpisy. Toto rozhodnutí bylo učiněno na základě jednání, která se uskutečnila během čtení návrhu v rámci Horizontální pracovní skupiny pro otázky týkající se kybernetiky, jakož i na základě skutečnosti, že s přihlédnutím ke konkrétnímu odkazu na tuto problematiku uvedenému v závěrech Rady ze dne 22. března týkajících se strategie kybernetické bezpečnosti EU pro digitální dekádu členské státy tuto otázku již označily za důležitou. Členské státy byly požádány, aby do 14. května 2021 předložily konkrétní návrhy znění k této otázce.

22. V průběhu portugalského předsednictví Horizontální pracovní skupina pro otázky týkající se kybernetiky dosud věnovala prezentaci návrhu a jeho čtení celkem 17 zasedání. Během těchto jednání uvedly některé členské státy výhradu přezkumu k celému návrhu nebo jeho částem.
23. Předsednictví je přesvědčeno, že pečlivé čtení revidované směrnice o bezpečnosti sítí a informací členským státům umožnilo získat od Komise podrobné vysvětlení nejvýznamnějších změn, jež byly v revidované směrnici provedeny, a současně zdůraznit své hlavní obavy týkající se návrhu, čímž se usnadní a zefektivní budoucí práce směřující ke včasnému dosažení obecného přístupu.

III. VĚCNÉ ASPEKTY

24. V diskuzích vedených v rámci Horizontální pracovní skupiny pro otázky týkající se kybernetiky členské státy revidovanou směrnici o bezpečnosti sítí a informací obecně uvítaly a upozornily na řadu klíčových otázek a obav, které by měly být během jednání o návrhu zohledněny.
25. Jednou z otázek, které byly během diskuzí opakovaně položeny, byla interakce revidované směrnice o bezpečnosti sítí a informací a odvětvových právních předpisů. Převážná většina členských států během dosavadních jednání uvedla, že je zcela nezbytné, aby se návrh revidované směrnice o bezpečnosti sítí a informací považoval za horizontální rámec pro kybernetickou bezpečnost v EU, a že by tento návrh měl sloužit jako základní norma pro minimální harmonizaci všech příslušných odvětvových právních předpisů v této oblasti.
26. Zadruhé byla vyjádřena řada obav plynoucích z významného rozšíření oblasti působnosti revidované směrnice o bezpečnosti sítí a informací týkajících se: rozsahu základních a důležitých subjektů spadajících do oblasti působnosti směrnice; odpovědnosti členských států za určení základních a důležitých subjektů; dopadů na schopnost příslušných vnitrostátních orgánů tyto seznamy subjektů sledovat; zvláštností příloh uvádějících podrobné informace o základních a důležitých subjektech spadajících do oblasti působnosti, např. široké začlenění potravinářského odvětví a odvětví dopravy bez ohledu na jejich význam pro příslušné odvětví; limitů souvisejících se zavedením velikostního omezení, zejména pokud jde o subjekty, které poskytují více než jednu službu, nebo o malé subjekty a mikrosubjekty se silnou vzájemnou závislostí na jiných službách, což má za následek dominové účinky.

27. Zatřetí některé členské státy, které by v souhrnu daly přednost přístupu založenému na posouzení rizik nebo dalším kvalitativním kritériím zavedeným na vnitrostátní úrovni, rovněž navrhly, aby oblast působnosti směrnice také zahrnovala kritéria velikostního omezení, která by při určování základních a důležitých subjektů představovala jediný prvek ke zvážení. Komise jasně uvedla, že kritéria velikostního omezení jsou nejvhodnějším, třebaže nikoliv ideálním, ukazatelem, jenž řeší neefektivní proces identifikace vyplývající ze stávající směrnice o bezpečnosti sítí a informací, čímž se zamezí roztržitosti při uplatňování budoucího nástroje.
28. Některé členské státy vyslovily pochybnosti o tom, zda právní základ týkající se jednotného trhu (článek 114 SFEU) umožňuje zahrnout do oblasti působnosti revidované směrnice i veřejnou správu. Tři členské státy vyjádřily zájem o získání písemného stanoviska právní služby Rady k této záležitosti. Kromě toho byla zpochybněna kritéria pro určení subjektů veřejné správy (klasifikace územních statistických jednotek – NUTS).
29. Pátá záležitost, na niž během jednání několik členských států poukázalo, se týká otázek národní bezpečnosti a toho, jak v praxi z oblasti působnosti revidované směrnice vyloučit veřejné subjekty podílející se na udržování veřejné bezpečnosti, obrany a národní bezpečnosti.
30. Další otázky, které vzbudily u členských států zájem, se týkaly vazeb a možných duplicit mezi různými strukturami, sítěmi a mechanismy v oblasti kybernetické bezpečnosti na úrovni EU, zejména v souvislosti se zavedením sítě EU-CyCLONe, ale také v návaznosti na očekávané připravované návrhy nebo iniciativy, jako např. zřízení sítě bezpečnostních operačních středisek (SOC) či návrh týkající se společné kybernetické jednotky.
31. Pokud jde o zavedení vzájemných hodnocení, některé členské státy vyjádřily pochybnosti ohledně povinné povahy tohoto úkonu a mechanismu pro zavedení příslušné metodiky, vnesly dotazy týkající se důvěrnosti a dostupnosti vyměňovaných informací a poukázaly na nedostatek zdrojů, které jsou k provádění těchto hodnocení k dispozici, zejména v menších členských státech.

32. Co se týče bezpečnosti dodavatelského řetězce, konkrétně opatření k řízení rizik v oblasti kybernetické bezpečnosti uvedených v článku 18 a koordinovaného posouzení rizik kritických dodavatelských řetězců v EU v článku 19 návrhu revidované směrnice, Komise uvedla, že v současné době zvažuje komplexní přístup, včetně případných nových horizontálních pravidel ke zlepšení kybernetické bezpečnosti všech propojených produktů a souvisejících služeb uváděných na vnitřní trh.
33. Jak bylo uvedeno výše, členské státy vznesly několik dotazů týkajících se koordinovaného zveřejňování informací o zranitelnostech a zřízení Evropského registru zranitelností agenturou ENISA. K těmto dvěma otázkám poskytla Komise podrobné informace a uvedla, že k jejich vývoji by došlo na základě stávajících vnitrostátních a mezinárodních osvědčených postupů a způsobů práce v této oblasti.
34. Pokud jde o oznamování, členské státy vyjádřily své názory na administrativní zátěž a z toho vyplývající dopady na odpovědnost, jakož i na 24hodinovou oznamovací lhůtu a oznamování související s významnými kybernetickými hrozbami a případy, kdy k incidentu téměř došlo.
35. Řada členských států, které požádaly Evropskou komisi o další objasnění těchto otázek, rovněž poukázala na praktická a právní hlediska týkající se zrušení příslušných ustanovení nařízení eIDAS a evropského kodexu pro elektronické komunikace.
36. Členské státy rovněž vyslovily pochybnosti ohledně rozsáhlých pravomocí, jež má mít dle revidované směrnice o bezpečnosti sítí a informací Komise v oblasti přijímání aktů v přenesené pravomoci a prováděcích aktů. To zahrnovalo dotazy týkajících se vazeb na akt o kybernetické bezpečnosti v souvislosti s certifikací.

IV. ZÁVĚRY

37. Předsednictví si velmi cení toho, že se Komise odhodlaně zapojila do procesu důkladného čtení, aby zodpověděla a objasnila dotazy a připomínky, jež během jednání vnesly členské státy.
38. Předsednictví dále oceňuje odhodlání členských států v rámci tohoto procesu, jež se projevilo řadou podrobných připomínek a otázek předložených během jednání. Předsednictví si je plně vědomo významného úsilí, které členské státy vynaložily z hlediska mezirezortní koordinace tohoto návrhu na vnitrostátní úrovni.
39. Na základě výše uvedených jednání v rámci Horizontální pracovní skupiny pro otázky týkající se kybernetiky je předsednictví přesvědčeno, že některé klíčové prvky návrhu revidované směrnice o bezpečnosti sítí a informací dosud nejsou dostatečně propracované, aby bylo možné úspěšně pokročit v jednáních mezi členskými státy o jejich návrzích. Předsednictví se proto domnívá, že vyřešení otázky interakce revidované směrnice o bezpečnosti sítí a informací s příslušnými odvětvovými právními předpisy umožní učinit pokrok v rámci tohoto návrhu a přispěje k nezbytnému vyjasnění příslušných odpovídajících ustanovení revidované směrnice o bezpečnosti sítí a informací a dalších právních aktů, které v současné době jsou nebo brzy budou projednávány v přípravných orgánech Rady (konkrétně například nařízení DORA a směrnice CER). Je rovněž třeba mít na paměti, že jednotlivé právní akty zahrnuté do této interakce se nacházejí v různých fázích procesu vyjednávání v rámci příslušných přípravných orgánů Rady. Řešení otázky interakce s příslušnými odvětvovými právními předpisy by v procesu přípravy revidované směrnice o bezpečnosti sítí a informací mělo ab initio umožnit hladký, nezávislý a řádný průběh jednání o různých právních aktech.

40. Podle současného plánování portugalského předsednictví uspořádá Horizontální pracovní skupina pro otázky týkající se kybernetiky do konce června 2021 celkem 19 zasedání věnovaných revidované směrnici o bezpečnosti sítí a informací. Předsednictví se domnívá, že dokončením důkladného a podle našeho názoru nezbytného čtení revidované směrnice a následným zahájením procesu vypracování návrhu Rada plně vyhověla výzvě Evropské rady učiněné na zasedání dne 26. února, aby urychleně pokročila v práci na revidované směrnici o bezpečnosti sítí a informací.
41. Portugalské předsednictví je odhodláno úzce spolupracovat s nastupujícím slovinským předsednictvím, aby usnadnilo pokračování jednání v rámci Horizontální pracovní skupiny pro otázky týkající se kybernetiky a zajistilo plynulý pokrok v souvislosti s tímto návrhem v Radě.
42. Vzhledem k výše uvedenému se Výbor stálých zástupců a Rada vyzývají, aby vzaly na vědomí pokrok, kterého bylo v projednávání navrhované směrnice dosaženo.
