Council of the European Union

Brussels, 10 March 2021
(OR. en, cs)

6890/21

Interinstitutional File:
2020/0365 (COD)

PROCIV 22	ENV 137
JAI 250	SAN 130
COSI 42	CHIMIE 28
ENFOPOL 85	RECH 93
CT 26	DENLEG 11
COTER 28	RELEX 181
ENER 69	HYBRID 11
TRANS 124	CYBER 58
TELECOM 92	ESPACE 14
ATO 16	INST 86
ECOFIN 231	PARLNAT 49

COVER NOTE

From:	Czech Parliament
date of receipt:	25 February 2021
To:	President of the Council of the EU
Subject:	Proposal for Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities [14262/20- COM(2020) 829 final] - Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find attached the above-mentioned document followed by a courtesy English translation.

Parlament České republiky

POSLANECKÁ SNĚMOVNA

2021

8. volební období

417.

USNESENÍ

výboru pro evropské záležitosti
z 65. schůze
ze dne 17. února 2021

ke společnému sdělení Evropskému parlamentu a Radě – Strategie kybernetické bezpečnosti EU pro digitální dekádu /kód Rady 14133/20, JOIN(2020) 18 v konečném znění/

k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 /kód Rady 14150/20, KOM(2020) 823 v konečném znění/

k návrhu směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů /kód Rady 14262/20, KOM(2020) 829 v konečném znění/

Výbor pro evropské záležitosti Poslanecké sněmovny Parlamentu ČR po vyslechnutí informace ředitele Národního úřadu pro kybernetickou a informační bezpečnost brig. gen. Ing. Karla Řehky, náměstka ministra vnitra JUDr. Jaroslava Strouhala, po vyslechnutí zpravodajské zprávy posl. Heleny Langšádlové a po rozpravě

s c h v a l u j e stanovisko, které je přílohou tohoto usnesení.

Jiří Valenta
ověřovatel

Helena Langšádlová
zpravodajka

František Kopřiva
místopředseda

Příloha k usnesení č. 417

Společné sdělení Evropskému parlamentu a Radě – Strategie kybernetické bezpečnosti EU pro digitální dekádu

JOIN(2020) 18 v konečném znění, kód Rady 14133/20

Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

KOM(2020) 823 v konečném znění, kód Rady 14150/20
Interinstitucionální spis 2020/0359/COD

Návrh směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů

KOM(2020) 829 v konečném znění, kód Rady 14262/20
Interinstitucionální spis 2020/0365/COD

- **Právní základ:**
  Článek 114 Smlouvy o fungování Evropské unie.

- **Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:**
  16. 1., 17. 12. a 18. 12. 2020

- **Datum projednání ve VEZ:**
  6. 1. 2021 (1. kolo)

- **Procedura:**
  Řádný legislativní postup.

- **Předběžné stanovisko vlády (dle § 109a odst. 1 jednacího řádu PS):**
  Datované dnem 1. 2. 2021 a 19. 1. 2021, doručené do výboru pro evropské záležitosti dne 28. 1. a 3. 2. 2021 prostřednictvím systému ISAP.

- **Hodnocení z hlediska principu subsidiarity:**
  Návrh je v souladu s principem subsidiarity.

- **Odůvodnění a předmět:**

Za účelem posílení kolektivní odolnosti Evropy proti kybernetickým hrozbám byla přijata Strategie kybernetické bezpečnosti EU pro digitální dekádu (dále jen „strategie“). Mnoho odvětví, mezi která patří například doprava, energetika a zdravotnictví, telekomunikace, bezpečnost či demokratické procesy, je do velké míry závislých na sítích a informačních systémech. Digitalizaci pracovních režimů navíc urychlila pandemie covidu-19.

Komise ve strategii představuje **tři hlavní nástroje, regulační, investiční a politické povahy**, **k řešení tří oblastí činnosti EU, kterými jsou: 1) odolnost, technologická suverenita a vedoucí postavení, 2) budování operační kapacity s cílem předcházet kybernetickým hrozbám, odrazovat od nich a reagovat na ně a 3) prosazování globálního a otevřeného kyberprostoru.**

Součástí opatření v oblasti zvyšování úrovně kybernetické bezpečnosti je Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148. Cílem návrhu je modernizovat stávající právní rámec a zohlednit zvýšenou digitalizaci vnitřního trhu a vyvíjející se prostředí kybernetických bezpečnostních hrozeb.

Komise také představila další opatření v oblasti zvyšování úrovně kybernetické bezpečnosti, kterým je Návrh směrnice Evropského parlamentu a Rady o odolnosti kritických subjektů. Cílem návrhu je reagovat na některé problémy v oblasti ochrany kritické infrastruktury v EU, přičemž nově se směrnice vztahuje na subjekty v deseti odvětvích, mezi která patří energetika, doprava, bankovnictví, zdravotnictví, pitná voda či například veřejná správa a vesmír.

- **Obsah a dopad:**

Komise ve strategii předně konstatuje, že kybernetická bezpečnost je nedílnou součástí bezpečnosti Evropanů. **Hrozby jsou podle Komise rovněž spojeny s geopolitickým napětím ohledně globálního a otevřeného internetu a souvisejí s kontrolou technologií v celém dodavatelském řetězci**. Za závažné globální riziko Komise považuje také **zacílení nepřátelské činnosti na kritickou infrastrukturu**, kdy zvýšené používání internetu v důsledku pandemie covidu-19 odhalilo křehkost dodavatelských řetězců závislých na digitální infrastruktuře. Komise dále upozorňuje na **obavy o bezpečnost, které jsou velkou překážkou používání on-line služeb**. Komise uvádí, že dvě pětiny uživatelů v EU zažily problémy související s bezpečností a tři pětiny mají dojem, že se nedokážou chránit před kyberkriminalitou.

Za účelem zajištění globálního a otevřeného internetu se silnou ochranou k řešení rizik pro bezpečnost a základních práv **Komise představuje tři hlavní nástroje, které jsou regulační, investiční a politické povahy**. Uvedené nástroje mají sloužit **k řešení tří oblastí činnosti EU, kterými jsou odolnost, technologická suverenita a vedoucí postavení, budování operační kapacity s cílem předcházet, odrazovat a reagovat a prosazování globálního a otevřeného kyberprostoru.**

Oddíl I - ODOLNOST, TECHNOLOGICKÁ SUVERENITA A VEDOUCÍ POSTAVENÍ

PRIORITY	PŘÍKLADY
ODOLNÁ INFRASTRUKTURA	revize směrnice o bezpečnosti sítí a inf. systémů
EVROPSKÝ KYBERNETICKÝ ŠTÍT	síť bezpečnostních operačních středisek
KOMUNIKAČNÍ INFRASTRUKTURA	pozemní sítě a vesmírné družice
NOVÉ GENERACE SÍTÍ	soubor nástrojů pro sítě 5G
INTERNET ZABEZPEČNÝCH VĚCÍ	akt o kybernetické bezpečnosti
GLOBÁLNÍ INTERNETOVÁ BEZPEČNOST	veřejná evropská služba pro překlad DNS
TECHNOLOGICKÝ DODAVATELSKÝ ŘETĚZEC	podpora průmyslové strategie
ZNALOSTI PRACOVNÍ SÍLY EU	revidovaný akční plán digitálního vzdělávání

1. priorita: Odolná infrastruktura a kritické služby

Komise navrhuje změnit pravidla EU, která se týkají bezpečnosti sítí a informačních systémů, v rámci revidované směrnice o bezpečnosti sítí a informačních systémů s cílem zvýšit úroveň kybernetické odolnosti všech příslušných veřejných i soukromých odvětví.

Komise dále navrhne opatření, včetně „kodexu sítě“, která stanoví pravidla pro kybernetickou bezpečnost přeshraničních toků elektřiny a bude pokračovat v prohlubování strategie kybernetické bezpečnosti systému Galileo.

2. **priorita: Budování evropského kybernetického štítu**

Komise navrhuje vybudovat síť bezpečnostních operačních středisek po celé EU a podporovat zdokonalování středisek stávajících i zakládání nových. Síť bude poskytovat včasná varování o kybernetických bezpečnostních incidentech orgánům a všem zúčastněným stranám a bude sloužit jako skutečný štít kybernetické bezpečnosti pro EU.

3. **priorita: Vysoce bezpečná komunikační infrastruktura**

Komise připomíná závazek členských států na zavedení zabezpečené kvantové komunikační infrastruktury pro Evropu. Tato infrastruktura bude mít dvě hlavní součásti, kterými jsou stávající pozemní komunikační sítě s optickými vlákny spojující strategická místa na vnitrostátní a přeshraniční úrovni a propojené vesmírné družice pokrývající celou EU.

4. **priorita: Zabezpečení nové generace širokopásmových mobilních sítí**

Podle Komise by občané EU a společnosti využívající pokročilé aplikace umožněné sítěmi 5G a příštími generacemi sítí měli mít rovněž nejvyšší standard zabezpečení. Členské státy s Komisí zavedly v lednu 2020 soubor nástrojů v rámci komplexního a objektivního přístupu ke kybernetické bezpečnosti sítí 5G.

5. **priorita: Internet zabezpečených věcí**

Komise již pracuje na zajištění transparentních bezpečnostních řešení a certifikace podle aktu o kybernetické bezpečnosti. Komise dále zváží komplexní přístup, včetně možných nových horizontálních pravidel„ například povinnost řádné péče pro výrobce zařízení připojených k internetu. Uvedená pravidla by dále posílila iniciativu „právo na opravu zastaralého softwaru“ představenou v akčním plánu pro oběhové hospodářství a doplnila by probíhající opatření ke konkrétním typům produktů, i ve vztahu ke kybernetické bezpečnosti pro motorová vozidla, a to u všech nových typů vozidel od července 2022.

6. **priorita: Větší globální internetová bezpečnost**

Komise má v úmyslu vypracovat pohotovostní plán podporovaný financováním EU pro řešení extrémních scénářů ovlivňujících integritu a dostupnost globálního kořenového systému DNS. Komise také přispěje k zabezpečenému připojení k internetu podporou rozvoje **veřejné evropské služby pro překlad DNS**. **Komise** dále ve spolupráci s členskými **státy urychlí zavádění klíčových internetových standardů včetně IPv6 a zavedených standardů zabezpečení internetu a osvědčených postupů pro zabezpečení DNS, směrování a e-mailů.**

7. **priorita: Posílená přítomnost v technologickém dodavatelském řetězci**

Komise se domnívá, že EU má jedinečnou příležitost spojit svá aktiva s cílem podpořit svou průmyslovou strategii a vedoucí postavení v oblasti digitálních technologií a kybernetické bezpečnosti v celém digitálním dodavatelském řetězci. Investice ze strany členských států by měly doplnit investice ze strany průmyslu v navrhovaném **průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti koordinačních center** (CCCN). Komise podpoří rozvoj specializovaného magisterského programu v oblasti kybernetické bezpečnosti a přispěje ke společnému evropskému plánu pro výzkum a inovace v oblasti kybernetické bezpečnosti.

8. **priorita: Pracovní síla EU se znalostí kybernetické bezpečnosti**

Podle Komise je nutné zvýšit informovanost o kybernetické bezpečnosti, k čemuž přispěje revidovaný akční plán digitálního vzdělávání. Komise rovněž společně s Úřadem EU pro duševní vlastnictví v rámci Europolu, s agenturou ENISA, členskými státy a soukromým sektorem vypracuje nástroje pro zvyšování povědomí a **pokyny ke zvýšení odolnosti podniků v EU proti krádežím duševního vlastnictví, které jsou způsobené kybernetickými útoky**.

EU by proto měla zajistit:

- přijetí revidované směrnice o bezpečností sítí a informací;
- regulační opatření pro internet zabezpečených věcí;
- investice do kybernetické bezpečnosti ve výši až 4,5 miliardy EUR;
- síť bezpečnostních operačních středisek EU s umělou inteligencí a maximálně bezpečnou komunikační infrastrukturu, která využívá kvantové technologie;

Oddíl II – BUDOVÁNÍ PROVOZNÍCH KAPACIT V OBLASTI PREVENCE, ODRAZOVÁNÍ A REAKCE

Cílem EU je podle Komise podporovat členské státy prostřednictvím plného provedení regulačních nástrojů, mobilizace a spolupráce. Za předcházení kybernetickým hrozbám a reakci na ně odpovídá několik komunit, mezi které patří orgány pro bezpečnost sítí a informací (například týmy CSIRT), donucovací a soudní orgány, kybernetická diplomacie a kybernetická obrana.

PRIORITY	PŘÍKLADY
SPOLEČNÁ KYBERNETICKÁ JEDNOTKA	vytvořit společné zázemí
POTÍRÁNÍ KYBERNETICKÉ KRIMINALITY	návrhy o elektronických důkazech
DIPLOMACIE	pracovní skupina pro kybernetické zpravodajské informace
KYBERNETICKÁ OBRANA	akční plán pro součinnost mezi civilním, obranným a kosmickým průmyslem

1. **priorita: Společná kybernetická jednotka**

Komise uvádí, že důležitým krokem k dokončení evropského rámce pro řešení kybernetických bezpečnostních krizí je společná kybernetická jednotka, která by měla umožnit plně využívat stávající struktury, zdroje a schopnosti a podporovat **potřebu sdílení.** Tímto způsobem by bylo možné odstranit **dva hlavní nedostatky, spočívající jednak v absenci společného prostoru komunit z civilní sféry, diplomatické oblasti a oblasti vymáhání práva a obrany a jednak v neschopnosti plně využít potenciálu operativní spolupráce a vzájemné pomoci v rámci stávajících sítí a komunit.**

Komise bude dále ve spolupráci s členskými státy a orgány a institucemi EU prosazovat **přírůstkový a inkluzivní přístup**.

2. **priorita: Potírání kybernetické kriminality**

Podle Komise má vyšetřování téměř všech typů trestné činnosti nějakou digitální složku. Komise bude využívat všech vhodných prostředků, včetně řízení o nesplnění povinnosti, aby zajistila plné provedení směrnice o útocích na informační systémy. Komise bude důsledněji předcházet zneužívání doménových jmen, a to i případnému šíření nezákonného obsahu, a bude usilovat o zajištění dostupnosti přesných údajů o registraci. Evropský parlament a Rada by rovněž měly rychle přijmout návrhy o elektronických důkazech.

3. **priorita: Soubor nástrojů pro diplomacii v oblasti kybernetiky**

K předcházení nepřátelské kybernetické činnosti a reakci na ni EU používá také svůj **soubor nástrojů pro diplomacii v oblasti kybernetiky**. Vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku podpoří a usnadní zřízení **pracovní skupiny členských států EU pro kybernetické zpravodajské informace**, sídlící ve Středisku EU pro analýzu zpravodajských informací (INTCEN), s cílem rozvíjet strategickou zpravodajskou spolupráci v dané oblasti.

4. **priorita: Posílení schopností v oblasti kybernetické obrany**

Vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku má ve spolupráci s Komisí předložit **přezkum politického rámce EU pro kybernetickou obranu**. K vymezení kybernetického prostoru jako oblasti operací přispěje **Vojenská vize a strategie pro kyberprostor jako oblast operací** a rovněž **vojenská síť CERT**, zřízená Evropskou obrannou agenturou. Komise také v prvním čtvrtletí 2021 předloží **akční plán pro součinnost mezi civilním, obranným a kosmickým průmyslem.**

EU by proto měla zajistit:

- dokončení evropského rámce pro řešení kybernetických bezpečnostních krizí;
- podporu a usnadnění zřízení pracovní skupiny členských států pro kybernetické zpravodajské informace v rámci Střediska EU pro analýzu zpravodajských informací;
-
- usnadnění rozvoje „Vojenské vize a strategie pro kyberprostor jako oblast operací“ EU pro účely vojenských misí a operací společné bezpečnostní a obranné politiky;
- podporu součinnosti mezi civilním, obranným a kosmickým průmyslem;
- posílení kybernetické bezpečnosti kritických kosmických infrastruktur v rámci kosmického programu.
-

Oddíl III – PROSAZOVÁNÍ GLOBÁLNÍHO A OTEVŘENÉHO KYBERPROSTORU

Mezinárodní spolupráce je podle Komise nezbytná pro udržení globálního, otevřeného, stabilního a bezpečného kyberprostoru. EU má rovněž jedinečné předpoklady k tomu, aby stála v čele procesu vymezování a prosazování mezinárodních standardů a norem.

PRIORITY	PŘÍKLADY
VEDOUCÍ POSTAVENÍ EU	ochrana a prosazování lidských práv a základních svobod
SPOLUPRÁCE S PARTNERY	neformální síť EU kybernetické diplomacie
POSÍLENÍ GLOBÁLNÍCH KAPACIT	Rada EU pro budování kybernetických kapacit

1. **priorita: Vedoucí postavení EU v oblasti standardů, norem a rámců v kybernetickém prostoru**

Komise se domnívá, že se **EU musí ve větší míře podílet na procesech stanovování mezinárodních norem a ve větší míře se v této oblasti ujímat vedení a posílit své zastoupení** v mezinárodních a evropských orgánech a v organizacích působících v oblasti vytváření standardů. EU má dále **prosazovat respektování mezinárodního práva**, zejména Charty Organizace spojených národů, a **má prosazovat, koordinovat a posilovat postoje členských států na mezinárodních fórech a vypracovat svůj vlastní postoj k uplatňování mezinárodního práva v kybernetickém prostoru**.

Podle Komise **EU nadále podporuje třetí země, které si přejí přistoupit k Budapešťské úmluvě Rady Evropy o počítačové kriminalitě**, a pokračuje v práci na dokončení **Druhého dodatkového protokolu k Budapešťské úmluvě**.

2. **priorita: Spolupráce s partnery a komunitou více zúčastněných stran**

EU by dále měla posílit a rozšířit své dialogy se třetími zeměmi o otázkách kybernetické bezpečnosti a ve spolupráci s delegacemi EU **vybudovat po celém světě neformální síť EU pro kybernetickou diplomacii.**

3. **priorita: Posílení globálních kapacit pro zvýšení globální odolnosti**

Komise také uvádí, že **EU by měla vypracovat agendu pro budování vnějších kybernetických kapacit a ke sledování dosaženého pokroku se zřídí Rada EU pro budování kybernetických kapacit.**

EU by proto měla zajistit:

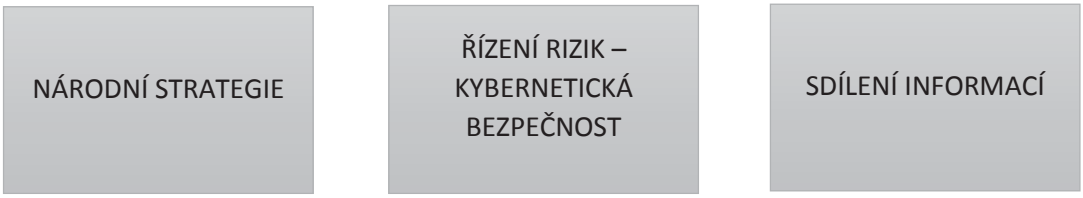
- lepší ochranu dětí před pohlavním zneužíváním a vykořisťováním;
- posílení a prosazování Budapešťské úmluvy o počítačové kriminalitě;
- rozšíření kybernetického dialogu EU s třetími zeměmi a s regionálními a mezinárodními organizacemi;
- navržení agendy EU pro budování vnějších kybernetických kapacit a Rady pro budování kybernetických kapacit EU.

Komise dále ve strategii upozorňuje na potřebu **kybernetické odolnosti u orgánů, institucí a agentur a potřebu bezpečnosti informací**, přičemž **Komise v roce 2021 předloží návrhy společných závazných pravidel pro bezpečnost informací a společných závazných pravidel pro kybernetickou bezpečnost.**

Ke strategickým iniciativám proto Komise řadí:

- nařízení o bezpečnosti informací v orgánech, institucích a agenturách EU;
- nařízení o společných pravidlech kybernetické bezpečnosti pro orgány, instituce a agentury EU;
- nový právní základ pro skupinu CERT EU za účelem posílení jejího mandátu a financování.

Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 se dotýká následujících oblastí:



1. **Ukládá členským státům povinnost přijmout národní strategie kybernetické bezpečnosti, určit příslušné vnitrostátní orgány, jednotná kontaktní místa a bezpečnostní týmy typu CSIRT** (čl. 5 – 11 navrhované směrnice).

- Národní strategie kybernetické bezpečnosti zahrnuje zejména definici cílů a priorit, správní rámec, hodnocení, určení opatření zajišťujících připravenost, reakci a obnovu při incidentech, seznam různých orgánů a subjektů zapojených do provádění národní strategie, politický rámec pro lepší koordinaci mezi příslušnými orgány.
- Národní strategie kybernetické bezpečnosti vymezují mimo jiné politiku zabývající se kybernetickou bezpečností v dodavatelském řetězci pro produkty a služby informačních a komunikačních technologií, pokyny týkající se zařazení a specifikace požadavků na kybernetickou bezpečnost produktů a služeb informačních a komunikačních technologií, politiku týkající se udržení celkové dostupnosti a integrity veřejného jádra otevřeného internetu či politiku řešící zvláštní potřeby malých a středních podniků.
- Členské státy mají Komisi oznámit národní strategie kybernetické bezpečnosti do tří měsíců od jejich přijetí a posuzovat je mají alespoň každé čtyři roky podle klíčových ukazatelů výkonnosti.
- Členské státy určí jeden nebo více orgánů odpovědných za kybernetickou bezpečnost a úkoly dohledu. Každý stát také určí jednotné kontaktní místo pro kybernetickou bezpečnost, které plní styčnou funkci pro účely přeshraniční spolupráce. Určení příslušného orgánu a jednotného kontaktního místa neprodleně oznámí Komisi.
- Každý členský stát zřídí jeden nebo více bezpečnostních týmů typu CSIRT, které pokrývají odvětví, pododvětví nebo subjekty uvedené v přílohách směrnice a jsou odpovědné za řešení incidentů.

2. **Stanovuje povinnost řízení rizik v oblasti kybernetické bezpečnosti a oznamovací povinnost pro subjekty vymezené v přílohách směrnice** (čl. 17 až 20 navrhované směrnice).

- Členské státy zajistí, aby vedoucí orgány základních a důležitých subjektů schválily opatření k řízení rizik v oblasti kybernetické bezpečnosti. Členové vedoucího orgánu mají pravidelně absolvovat zvláštní školení, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika.
- Základní a důležité subjekty mají přijmout vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, mezi která patří analýza rizik a politika bezpečnosti informačních systémů, řešení incidentů, řízení kontinuity provozu a krizové řízení či používání kryptografie a šifrování.
- U kritických dodavatelských řetězců v EU může skupina pro spolupráci s Komisí a Agenturou ENISA provést koordinované posouzení rizik.
- Základní a důležité subjekty mají neprodleně oznamovat příslušným orgánům nebo týmu CSIRT každý incident, který má závažný dopad na poskytování jejich služeb, stejně jako každou významnou kybernetickou hrozbu, kterou zjistí a která by mohla mít za následek významný incident.

3. **Stanovuje povinnosti týkající se sdílení informací o kybernetické bezpečnosti** (čl. 26 a 27 navrhované směrnice).

- Členské státy zajistí, aby základní a důležité subjekty mohly mezi sebou sdílet podstatné informace o kybernetické bezpečnosti.
- Členské státy zajistí, aby k výměně informací docházelo v důvěryhodných komunitách základních a důležitých subjektů.
- Členské státy rovněž zajistí, aby subjekty, které nespadají do oblasti působnosti této směrnice, mohly dobrovolně oznamovat významné incidenty, kybernetické hrozby nebo případy, kdy téměř došlo k incidentu.

Návrh směrnice rovněž obsahuje ustanovení o skupině pro spolupráci (čl. 12), síti CSIRT (čl. 13), Evropské síti styčných organizací pro řešení kybernetických krizí (čl. 14), zprávě o stavu kybernetické bezpečnosti (čl. 15), vzájemných hodnoceních (čl. 16), použití evropských systémů certifikace kybernetické bezpečnosti (čl. 21), standardizaci (čl. 22), databázi doménových jmen a registračních údajů (čl. 23) a ustanovení k pravomoci a registraci (čl. 24 a 25), ustanovení o dohledu a vymáhání (čl. 28 až 34). V přechodných a závěrečných ustanoveních je vymezen přezkum a výkon přenesené pravomoci.

Návrh směrnice Evropského parlamentu a Rady o odolnosti kritických subjektů se dotýká následujících oblastí:

1. **Národní rámec k odolnosti kritických subjektů** (čl. 3 – 9 navrhované směrnice)

- Členské státy by měly přijmout strategie pro posílení odolnosti kritických subjektů. Tyto strategie by měly obsahovat mimo jiné strategické cíle a priority, správní rámec k dosažení těchto cílů a priorit, popis nezbytných opatření a politický rámec. Strategie by měla být alespoň každé čtyři roky aktualizována.
- Příslušné orgány vytvoří seznam podstatných služeb v sektorech uvedených v příloze. Členské státy mají Komisi poskytnout údaje o identifikovaných druzích rizik a výsledcích posouzení rizik pro sektory a subsektory vymezené v příloze.
- Členské státy rovněž určí jeden nebo více příslušných orgánů, které odpovídají za správné uplatňování pravidel, a dále určí jednotné kontaktní místo.

2. **Odolnost kritických subjektů** (čl. 10 – 13 navrhované směrnice)

- Členské státy zajistí, aby kritické subjekty posoudily do šesti měsíců po obdržení oznámení a, je-li to nutné, také každé čtyři roky, všechna relevantní rizika, která mohou narušit jejich provoz.
- Kritické subjekty přijmou vhodná a přiměřená technická a organizační opatření k zajištění své odolnosti.
- Kritické subjekty mají bez zbytečného odkladu informovat příslušný orgán o událostech, které významně narušují nebo mohou významně narušit jejich provoz.

3. **Zvláštní dohled nad kritickými subjekty zvláštního evropského významu** (čl. 14 a 15 navrhované směrnice)

- Kritické subjekty zvláštního evropského významu jsou pod zvláštním dohledem.

4. **Spolupráce a oznamování** (čl. 16 navrhované směrnice)

- Za účelem výměny informací a ke strategické spolupráci je zřízena skupina odolnosti kritických subjektů, které předsedá zástupce Komise.

Směrnice rovněž obsahuje ustanovení o dohledu a vymáhání (čl. 18) a sankcích (čl. 19) a v závěrečných ustanoveních (čl. 20 až 26) mimo jiné pravomoc Komise přijímat akty v přenesené působnosti či podávání zpráv Evropskému parlamentu a Radě.

- **Stanovisko vlády ČR:**
  Vláda novou strategii kybernetické bezpečnosti vítá, zejména její vysokou míru integrace kybernetické bezpečnosti a související mezinárodní vztahy. Vláda rovněž oceňuje lidskoprávní aspekty a demokratické hodnoty obsažené ve strategii, nicméně uvítala by větší důraz na osvětu v oblasti kybernetické bezpečnosti, principy digitální hygieny a intenzivnější strategickou komunikaci. Dále vláda vítá důraz kladený na investice do kybernetické bezpečnosti jako předpoklad technologického rozvoje, postrádá však explicitnější podporu využití unijních financí pro účely poskytování pomoci třetím zemím.

Vláda dále vítá snahu zvýšit úroveň kybernetické bezpečnosti napříč Unií prostřednictvím směrnice o opatřeních k zajištění vysoké společné kybernetické bezpečnosti v Unii, nicméně se domnívá, že nejsou plně respektovány zásady subsidiarity a proporcionality nezbytné pro výkon pravomocí. Podle jejího názoru není členským státům ponechán dostatečný prostor pro vnitrostátní úpravu, což by bylo vhodnější s ohledem na lepší znalost konkrétní problematiky a národních poměrů a s ohledem na národní specifika. S ohledem na zásah do národní bezpečnosti je ingerence Unie v některých oblastech přímo nežádoucí.

Vláda chápe snahu Komise revidovat současný přístup spojený s ochranou kritických subjektů, nicméně nesouhlasí s navrhovanou formou právního nástroje. **Návrh směrnice odolnosti kritických subjektů podle vlády porušuje principy subsidiarity a proporcionality a dotýká se oblasti vnitřní bezpečnosti a civilní ochrany, kde je harmonizace vyloučena.** Směrnice by výrazně zvýšila administrativní zátěž a byla by spojena s náklady na finanční a personální zajištění. Navrhované finanční prostředky jsou přitom určeny převážně na aktivity Komise. Vláda rovněž nesouhlasí s rozšířeným výběrem odvětví, neboť navrhovaná odvětví jsou řešena různými relevantními národními či evropskými předpisy.

- **Předpokládaný harmonogram projednávání v orgánech EU:**
  Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 je v současné době v prvním čtení v Radě EU.

  Návrh směrnice Evropského parlamentu a Rady o odolnosti kritických subjektů je v současné době v prvním čtení v Radě EU.

- **Závěr:**

  Výbor pro evropské záležitosti

  1. **b e r e n a v ě d o m í** společné sdělení Evropskému parlamentu a Radě – Strategie kybernetické bezpečnosti EU pro digitální dekádu /kód Rady 14133/20, JOIN(2020) 18 v konečném znění/;

  2. **b e r e n a v ě d o m í** návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 /kód Rady 14150/20, KOM(2020) 823 v konečném znění/;

  3. **b e r e n a v ě d o m í** návrh směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů /kód Rady 14262/20, KOM(2020) 829 v konečném znění/;

  4. **p o d p o r u j e** rámcové pozice vlády k těmto dokumentům;

  5. **v í t á** nejen plánované navýšení unijních investic do technologií a kapacit kybernetické bezpečnosti, ale zejména důraz na kyberbezpečnost z pohledu zahraničně-politického;

6. **u p o z o r ň u j e ,** že v ČR by tímto došlo k podstatnému nárůstu počtu regulovaných subjektů. Míra významnosti těchto subjektů z bezpečnostního hlediska by se přitom do značné míry lišila. Z pohledu ČR je proto nutné k regulaci kybernetické bezpečnosti podle NIS 2 přistupovat s důrazem na zásady proporcionality a subsidiarity, a to zejména zohledněním toho, jaké dopady na fungování státu a potřeby společnosti by kybernetický incident u určitého subjektu mohl způsobit;

7. **b y u v í t a l** větší důraz na osvětu v oblasti kybernetické bezpečnosti, principy digitální hygieny a intenzivnější strategickou komunikaci, stejně tak jako vyšší podporu využití unijních financí pro účely poskytování pomoci třetím zemím;

8. **d o p o r u č u j e** přehodnotit, zda finanční a administrativní náklady odpovídají přiměřeně cílům zvýšení odolnosti kritických subjektů;

9. **p o v ě ř u j e** předsedu výboru pro evropské záležitosti, aby v rámci politického dialogu postoupil toto usnesení předsedkyni Evropské komise.

Jiří Valenta
ověřovatel

Helena Langšádlová
zpravodajka

František Kopřiva
Místopředseda

Courtesy translation

PARLIAMENT
OF THE CZECH REPUBLIC
Chamber of Deputies
Ondřej Benešík
Chairman
Committee on European Affairs

Prague, 23rd February 2021

Dear Ms. President,

I would like to inform you about the opinion of the Committee on European Affairs of the Chamber of Deputies of the Parliament of the Czech Republic

on the Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade /Council Code 14133/20, JOIN(2020)18 final/;

on the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 /Council Code 14150/20, COM(2020)823 final/ and

on the Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities /Council Code 14262/20, COM(2020)829 final/.

The respective documents were included in the agenda of the 65th session of the Committee for European Affairs and was scrutinized on 17th February 2021. According to the Rules of Procedure the Director of the National Office for Cyber and Information Security and the Deputy Minister of the Interior were present at the session to introduce the preliminary Government's Framework Position.

After the hearing of the rapporteur's review and after the discussion the Committee has adopted the resolution No. 417 **in the context of the Political Dialogue** which is enclosed to this letter.

Yours sincerely

Enclosure

Ms. Ursula von der Leyen
President of the European Commission
B r u s s e l s

Parliament of the Czech Republic, Chamber of Deputies, Sněmovní 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez

PARLIAMENT OF THE CZECH REPUBLIC
Chamber of Deputies
Committee on European Affairs

Resolution No. 417

65th Session on 17 February 2021

Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade /Council Code 14133/20, JOIN(2020)18 final/;

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 /Council Code 14150/20, COM(2020)823 final/;

Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities /Council Code 14262/20, COM(2020)829 final/

Conclusions of the Resolution:

Committee for European Affairs

1. **takes note of** the Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade /Council Code 14133/20, JOIN(2020)18 final/;
2. **takes note of** the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 /Council Code 14150/20, COM(2020)823 final/;
3. **takes note of** the Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities /Council Code 14262/20, COM(2020)829 final/;
4. **supports** the Government's Framework Positions on these documents;
5. **welcomes** not only the planned increase in EU investment in cybersecurity technologies and capabilities, but in particular the emphasis on cybersecurity from a foreign policy perspective;
6. **points out** that this would lead to a significant increase in the number of regulated entities in the Czech Republic. The level of importance of these entities from a security point of view would vary considerably. From the point of view of the Czech Republic, it is therefore necessary to regulate cyber security according to NIS 2 with emphasis on the principles of proportionality and subsidiarity, especially taking into account what impacts on the functioning of the state and society's needs could cause a cyber incident in a particular entity;
7. **would welcome** greater emphasis on cyber security awareness, digital hygiene principles and enhanced strategic communication, as well as greater support for the use of EU funds to provide assistance to third countries;
8. **recommends** a reassessment of whether the financial and administrative costs are commensurate with the objectives of increasing the resilience of critical entities;
9. **authorizes** the Chairman of the Committee on European Affairs to forward this resolution to the President of the European Commission **in the framework of the Political Dialogue.**

Parliament of the Czech Republic, Chamber of Deputies, Sněmovní 3, 118 26 Praha 1
tel.: +420-257 173 411, fax: +420-257 173 415
http://www.psp.cz/vez