Rada
Evropské unie

Brusel 9. března 2021
(OR. en)

6722/21

CYBER 55	RECH 86
JAI 227	COMPET 151
JAIEX 23	IND 52
EJUSTICE 25	COTER 25
COSI 39	ENFOPOL 80
DATAPROTECT 54	COPS 79
COPEN 103	MI 136
TELECOM 88	IXIM 43
PROCIV 21	POLMIL 25
CSC 85	HYBRID 10
CIS 35	CSCI 34
RELEX 168	POLGEN 33

POZNÁMKA K BODU „I/A“

Odesílatel:	Generální sekretariát Rady
Příjemce:	Výbor stálých zástupců / Rada
Předmět:	Návrh závěrů Rady týkajících se strategie kybernetické bezpečnosti EU pro digitální dekádu

1. Komise a vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku dne 16. prosince 2020 zveřejnili společné sdělení Evropskému parlamentu a Radě s názvem „Strategie kybernetické bezpečnosti EU pro digitální dekádu“[1]. Cílem nové strategie kybernetické bezpečnosti je posílit kolektivní odolnost Evropy vůči kybernetickým hrozbám a zajistit, aby všichni občané a podniky mohli plně využívat důvěryhodných a spolehlivých služeb a digitálních nástrojů.

[1] Dokument 14133/20.

2. Komise a ESVČ představily společné sdělení na neformální videokonferenci Horizontální pracovní skupiny pro otázky týkající se kybernetiky, jež se konala ve dnech 17. prosince 2020 a 12. ledna 2021. Na neformální videokonferenci Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 17. prosince 2020 nastupující portugalské předsednictví oznámilo svůj záměr vypracovat návrh závěrů Rady o strategii kybernetické bezpečnosti EU pro digitální dekádu.

3. První návrh závěrů Rady předložilo předsednictví na neformální videokonferenci Horizontální pracovní skupiny pro otázky týkající se kybernetiky dne 2. února 2021. Tyto závěry byly následně projednány na neformálních videokonferencích Horizontální pracovní skupiny pro otázky týkající se kybernetiky ve dnech 9. února 2021, 19. února 2021, 1. března 2021 a 9. března 2021.

4. Poněvadž návrh závěrů rovněž obsahuje odkaz na obranné politiky EU (bod 30), byl příslušný bod projednán na zasedání Politicko-vojenské skupiny dne 10. února 2021.

5. Různé body se týkají společné zahraniční a bezpečnostní politiky (body 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 a 33), a proto byly předloženy Politickému a bezpečnostnímu výboru, který tyto body potvrdil na svém zasedání dne 4. března 2021.

6. Horizontální pracovní skupina pro otázky týkající se kybernetiky dosáhla na neformální videokonferenci dne 9. března 2021 dohody o návrhu závěrů Rady ve znění uvedeném v dokumentu 6722/21.

7. S ohledem na výše uvedené skutečnosti se Výbor stálých zástupců vyzývá, aby návrh závěrů Rady ve znění uvedeném v příloze předložil Radě a navrhl jí, aby tento návrh závěrů přijala v rámci bodů „A“ pořadu jednání.

PŘÍLOHA

Návrh závěrů Rady týkajících se strategie kybernetické bezpečnosti EU pro digitální dekádu

RADA EVROPSKÉ UNIE,

PŘIPOMÍNAJÍC své závěry o:

– společném sdělení Evropskému parlamentu a Radě ze dne 25. června 2013 nazvaném Strategie kybernetické bezpečnosti Evropské unie: „Otevřený, bezpečný a chráněný kyberprostor“[2],

– správě internetu[3],

– společném sdělení Evropskému parlamentu a Radě ze dne 20. listopadu 2017: „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“[4],

– budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU[5],

– významu 5G pro evropské hospodářství a potřebě zmírnit bezpečnostní rizika spojená s 5G[6],

– budoucnosti vysoce digitalizované Evropy po roce 2020: „Posílení digitální a hospodářské konkurenceschopnosti v Unii a digitální soudržnosti“[7],

– dalším úsilí za účelem posílení odolnosti a boje proti hybridním hrozbám[8],

– utváření digitální budoucnosti Evropy[9],

---

2 Dokument 12109/13.
3 Dokument 16200/14.
4 Dokument 14435/17 + COR 1.
5 Dokument 7737/19.
6 Dokument 14517/19.
7 Dokument 9596/19.
8 Dokument 14972/19.
9 Dokument 8711/20.

– digitální diplomacii[10],

– posílení odolnosti a boji proti hybridním hrozbám, včetně dezinformací, v souvislosti s pandemií COVID-19[11],

– kybernetické diplomacii[12],

– koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[13],

– rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“)[14],

– pokynech EU pro budování vnějších kybernetických kapacit[15],

– oživení urychlujícím přechod k dynamičtějšímu, odolnějšímu a konkurenceschopnějšímu evropskému průmyslu[16],

– kybernetické bezpečnosti zařízení připojených k internetu[17],

– posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti[18],

– a své usnesení Rady o šifrování – bezpečnost prostřednictvím šifrování a bezpečnost navzdory šifrování[19],

---

10 Dokument 12804/20.
11 Dokument 14064/20.
12 Dokument 6122/15 + COR 1.
13 Dokument 10086/18.
14 Dokument 10474/17.
15 Dokument 10496/18.
16 Dokument 13004/20.
17 Dokument 13629/20.
18 Dokument 14540/16.
19 Dokument 13084/1/20 REV 1.

– a prohlášení členských států ze dne 15. října 2020 o budování cloudu nové generace pro podniky a veřejný sektor v EU“ (*Building the next generation cloud for businesses and the public sector in the EU*);

PŘIPOMÍNAJÍC závěry Evropské rady o COVID-19, jednotném trhu, průmyslové politice, digitálních aspektech a vnějších vztazích přijaté na zasedání ve dnech 1. a 2. října 2020[20], jakož i závěry Evropské rady o dezinformacích a hybridních hrozbách a o nové strategické agendě 2019–2024 přijaté na zasedání dne 20. června 2019[21];

PŘIPOMÍNAJÍC dokument ze dne 28. června 2016 s názvem „Globální strategie zahraniční a bezpečnostní politiky Evropské unie – Sdílená vize, společný postup: silnější Evropa“;

PŘIPOMÍNAJÍC sdělení Komise ze dne 19. prosince 2020 o formování digitální budoucnosti Evropy[22] a ze dne 24. července 2020 o strategii bezpečnostní unie EU[23];

PŘIPOMÍNAJÍC společné sdělení Evropské komise a vysokého představitele ze dne 2. prosince 2020 o nové agendě EU a USA pro globální změnu[24];

1. ZDŮRAZŇUJE, že kybernetická bezpečnost je základem pro budování odolné, zelené a digitální Evropy, a VÍTÁ společné sdělení Evropskému parlamentu a Radě s názvem „Strategie kybernetické bezpečnosti EU pro digitální dekádu“, jež nastiňuje nový rámec pro činnost EU v oblasti „odolnosti, technologické suverenity a vedoucího postavení“, jakož i to, jak má EU chránit své občany, podniky a orgány před kybernetickými incidenty a hrozbami a zároveň posilovat důvěru jednotlivců a organizací ve schopnost EU podporovat bezpečné a spolehlivé sítě a informační systémy, infrastrukturu a konektivitu a podporovat a chránit globální, otevřený, svobodný, stabilní a bezpečný kyberprostor vybudovaný na základě lidských práv, základních svobod, demokracie a právního státu.

---

20 Dokument EUCO 13/20.
21 Dokument EUCO 9/19.
22 19.2.2020 COM(2020) 67 final.
23 24.7.2020 COM(2020) 605 final.
24 2.12.2020 JOIN(2020) 22 final.

2. UZNÁVÁ, že vlivem pandemie COVID-19 se nedílnou součástí našeho každodenního života stala zvýšená potřeba důvěřovat nástrojům a systémům informačních a komunikačních technologií (IKT) a jejich bezpečnosti. ZDŮRAZŇUJE, že kybernetická bezpečnost a globální a otevřený internet mají zásadní význam jak pro fungování veřejné správy a veřejných orgánů na vnitrostátní i unijní úrovni, tak pro naši společnost a hospodářství jako celek.

3. ZDŮRAZŇUJE potřebu zvyšovat povědomí o kybernetických otázkách na politické a strategické úrovni rozhodování tím, že subjekty s rozhodovací pravomocí získají příslušné znalosti a informace, a VYZDVIHUJE potřebu zlepšovat informovanost široké veřejnosti a podporovat kybernetickou hygienu.

4. VYZÝVÁ k prosazování a ochraně základních hodnot EU, jimiž jsou demokracie, právní stát, lidská práva a základní svobody, včetně práva na svobodu projevu a informací, práva na svobodu shromažďování a sdružování a práva na soukromí v kyberprostoru. V tomto ohledu VÍTÁ další trvalé úsilí chránit obránce lidských práv a zástupce občanské společnosti a akademické obce zabývající se otázkami kybernetické bezpečnosti, ochrany údajů, dohledu a cenzury na internetu, a to vydáváním dalších praktických pokynů, podporou osvědčených postupů a intenzivnějším úsilím EU zamezit porušování a zneužívání lidských práv a zneužívání nově vznikajících technologií, především využíváním diplomatických opatření v nezbytných případech a kontrolou vývozu těchto technologií. V této souvislosti ZDŮRAZŇUJE význam akčního plánu EU pro lidská práva a demokracii na období 2020–2024 a obecných zásad EU v oblasti lidských práv ohledně svobody projevu online a offline.

5. PODTRHUJE, že klíčovým cílem Unie je dosáhnout strategické autonomie při současném zachování otevřené ekonomiky, aby si Unie sama určovala své ekonomické směřování a zájmy. To zahrnuje posílení schopnosti činit autonomní rozhodnutí týkající se kybernetické bezpečnosti, aby se upevnilo vedoucí postavení EU v digitální oblasti i její strategické kapacity. PŘIPOMÍNÁ, že k tomu je třeba určit a omezit strategické závislosti a zvýšit odolnost nejcitlivějších průmyslových ekosystémů a specifických oblastí. PODTRHUJE, že toto může zahrnovat diverzifikaci výrobních a dodavatelských řetězců, podporu a zatraktivnění investic a výroby v Evropě, hledání alternativních řešení a oběhových modelů a podporu široké průmyslové spolupráce napříč členskými státy.

6. Vzhledem k tomu, že se u pracovní síly projevuje nedostatek dovedností v oblasti digitálních technologií a kybernetické bezpečnosti, ZDŮRAZŇUJE, že je důležité uspokojit poptávku po pracovní síle, jež je vyškolena v oblasti digitálních technologií a kybernetické bezpečnosti, a to zejména rozvíjením, udržováním a získáváním největších talentů, například prostřednictvím vzdělávání a odborné přípravy, aby bylo možné naši společnost kyberneticky bezpečným způsobem digitalizovat. PODPORUJE vzdělávání většího počtu žen a dívek v oblasti přírodních věd, technologií, inženýrství a matematiky („STEM“) a prohlubování dovedností a změnu kvalifikace u pracovních míst v oblasti IKT se zaměřením na digitální dovednosti jako jeden ze způsobů, jak překlenout digitální propast mezi ženami a muži.

7. PŘIPOMÍNÁ, že cílem společného a komplexního přístupu EU ke kybernetické diplomacii je podílet se na předcházení konfliktům, zmírňování kybernetických hrozeb a větší stabilitě mezinárodních vztahů. V této souvislosti ZNOVU POTVRZUJE, že je odhodlána řešit mezinárodní spory v kyberprostoru mírovými prostředky a že veškeré diplomatické úsilí EU by mělo být přednostně zaměřeno na podporu bezpečnosti a stability v kyberprostoru prostřednictvím intenzivnější mezinárodní spolupráce, jakož i na snižování rizika plynoucího z nepochopení, eskalace a konfliktů, jež mohou být způsobeny incidenty v oblasti IKT, a PODPORUJE další rozvoj a provádění opatření na budování důvěry na regionální a mezinárodní úrovni. OPĚTOVNĚ POUKAZUJE na výzvu Valného shromáždění Organizace spojených národů, schválenou na základě konsensu, aby se členské státy OSN při využívání IKT řídily doporučeními uvedenými ve zprávách skupin vládních expertů, a ZNOVU ZDŮRAZŇUJE, že je třeba v kyberprostoru uplatňovat mezinárodní právo, zejména Chartu OSN v celém jejím rozsahu.

8. OPĚTOVNĚ ZDŮRAZŇUJE, že aby bylo možné mezinárodní normy a standardy v oblastech nově vznikajících technologií a technické a logické infrastruktury, jež je základem pro obecnou dostupnost a integritu veřejného jádra internetu, do značné míry utvářet tak, aby na základě mnohostranného přístupu byly v souladu s univerzálními hodnotami a hodnotami EU, je další rozvoj norem a standardů v rámci Unie zásadní. Tímto se zajistí, aby internet zůstal globální, otevřený, svobodný, stabilní a bezpečný, aby se při používání a vývoji digitálních technologií dodržovala lidská práva a aby se digitální technologie používaly ve shodě s právem, bezpečně a eticky. BERE NA VĚDOMÍ připravovanou strategii pro normalizaci a ZAVAZUJE SE, že bude aktivním a koordinovaným způsobem usilovat o prosazování vedoucí pozice a cílů EU na mezinárodní úrovni, a to i v různých mezinárodních normalizačních organizacích a prostřednictvím spolupráce s podobně smýšlejícími partnery, zástupci občanské společnosti, akademické obce a soukromého sektoru.

9. JEDNOZNAČNĚ PODPORUJE, aby se v otázce správy internetu a kybernetické bezpečnosti využíval model více zúčastněných stran, a zavazuje se, že i v souvislosti s pařížskou výzvou pro důvěru a bezpečnost v kyberprostoru posílí na mezinárodních fórech pravidelné a strukturované výměny informací se zúčastněnými stranami, včetně zástupců soukromého sektoru, akademické obce a občanské společnosti. PROSAZUJE univerzální, dostupný a rovný přístup k internetu, aby se překlenuly digitální propasti, a především posílení postavení žen a dívek a osob ve zranitelném postavení nebo na okraji zájmu společnosti, a to jak při rozvoji politik, tak při používání internetu.

10. ZDŮRAZŇUJE, že v nadcházejících letech je zapotřebí začlenit kybernetickou bezpečnost do digitálních investic a iniciativ a postupně se podílet na vytváření rovných podmínek v oblasti kybernetické bezpečnosti, a BERE NA VĚDOMÍ, že Komise hodlá zvýšit veřejné výdaje na kybernetickou bezpečnost a mobilizovat soukromé investice v této oblasti. POUKAZUJE NA význam malých a středních podniků v ekosystému kybernetické bezpečnosti a OCEŇUJE příslušné finanční nástroje, které jsou k dispozici a díky nimž se v rámci digitální transformace v průběhu víceletého finančního rámce (VFR) na období 2021–2027 i v Nástroji pro oživení a odolnost věnuje kybernetické bezpečnosti zvláštní pozornost.

11. SE ZÁJMEM OČEKÁVÁ rychlé provedení nařízení, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, s čímž souvisí rychlé zřízení a zprovoznění Evropského centra kompetencí pro kybernetickou bezpečnost v Bukurešti. Rychlé přijetí jeho programu přispěje k maximalizaci dopadu investic, jejichž účelem je posílit vedoucí postavení a strategickou autonomii Unie v oblasti kybernetické bezpečnosti, podpořit technologické kapacity a dovednosti a zvýšit globální konkurenceschopnost Unie s využitím vstupů od průmyslových subjektů a zástupců akademické obce zabývajících se kybernetickou bezpečností, včetně malých a středních podniků a výzkumných středisek, jež budou těžit ze systematičtější, přístupnější a strategičtější spolupráce zohledňující soudržnost Unie a všech jejích členských států.

12. VÍTÁ probíhající činnost pod vedením Agentury Evropské unie pro kybernetickou bezpečnost (ENISA), členských států a zúčastněných stran, jejímž cílem je poskytnout Evropské unii systémy certifikace produktů, služeb a procesů IKT, které by měly přispět ke zvýšení celkové úrovně kybernetické bezpečnosti v rámci jednotného digitálního trhu. V této souvislosti SE ZÁJMEM OČEKÁVÁ průběžný pracovní program Unie, a to s ohledem na vytvoření unijních systémů certifikace kybernetické bezpečnosti v souladu s aktem o kybernetické bezpečnosti. V této souvislosti UZNÁVÁ ústřední úlohu EU při vytváření norem, které mohou formovat oblast kybernetické bezpečnosti a přispívají k zajištění spravedlivé hospodářské soutěže na unijní i celosvětové úrovni, podporují přístup na trh, řeší bezpečnostní rizika a zároveň zajišťují použitelnost legislativního rámce EU.

13. OPĚTOVNĚ ZDŮRAZŇUJE, že je důležité posoudit, do jaké míry je zapotřebí horizontální právní předpis, upřesňující rovněž nezbytné podmínky pro uvedení na trh, jenž by z dlouhodobého hlediska řešil všechny příslušné aspekty kybernetické bezpečnosti zařízení připojených k internetu, jako je dostupnost, integrita a důvěrnost. VÍTÁ v tomto ohledu diskusi, jejímž účelem je zvážit oblast působnosti takového právního předpisu a jeho propojení s rámcem pro certifikaci kybernetické bezpečnosti podle definice uvedené v aktu o kybernetické bezpečnosti, a to s cílem zvýšit bezpečnost jednotného digitálního trhu. ZDŮRAZŇUJE, že aby se předešlo nejednoznačnosti a roztříštěnosti právní úpravy, požadavky na kybernetickou bezpečnost by měly být vymezeny v souladu s příslušnými právními předpisy Unie, včetně aktu o kybernetické bezpečnosti, nového legislativního rámce, nařízení o evropské normalizaci a případného nového horizontálního právního předpisu.

14. UZNÁVÁ, 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 BERE 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 potvrzuje, že podporuje posilování a harmonizaci vnitrostátních rámců kybernetické bezpečnosti a trvalé spolupráce mezi členskými státy. Dále ZDŮRAZŇUJE potřebu sladit a formulovat odvětvové právní předpisy v této oblasti.

15. BERE NA VĚDOMÍ návrh Komise podpořit členské státy při zřizování a posilování bezpečnostních operačních středisek (SOC) s cílem vybudovat síť SOC v celé EU a dále sledovat a na základě signálů předvídat útoky na sítě. V této souvislosti OČEKÁVÁ podrobné plány Komise týkající se sítě bezpečnostních operačních středisek, přičemž respektuje pravomoci členských států. PŘIPOMÍNÁ úsilí členských států zřídit za podpory EU odvětvové, vnitrostátní a regionální skupiny pro reakce na počítačové bezpečnostní incidenty (týmy CSIRT) a vnitrostátní či evropská střediska pro sdílení a analýzu informací (ISAC) jako součást účinné unijní sítě partnerství pro kybernetickou bezpečnost. Se ZÁJMEM OČEKÁVÁ prozkoumání toho, jaký má tato síť potenciál pro posílení bezpečnostních operačních středisek a jejich komplementaritu a koordinaci se stávajícími sítěmi a subjekty (zejména se sítí týmů CSIRT), aby se podpořila efektivní, bezpečná a spolehlivá kultura sdílení informací. ZDŮRAZŇUJE, že tento proces bude navazovat na činnost vykonanou v rámci iniciativ týkajících se umělé inteligence a vysoce výkonné výpočetní techniky a prostřednictvím evropských center pro digitální inovace.

16. BERE NA VĚDOMÍ možný rozvoj zabezpečeného systému připojení, jenž vychází z evropské kvantové komunikační infrastruktury (EuroQCI) a družicové komunikace v rámci státní správy Evropské unie (GOVSATCOM), a UZNÁVÁ, že jakýkoli možný rozvoj by měl být v budoucnu založen na spolehlivém rámci kybernetické bezpečnosti a měl by zohledňovat celou infrastrukturu elektronických komunikací, jako např. vesmírné, pozemní a podmořské systémy sítí.

17. Se ZÁJMEM OČEKÁVÁ jednání s Komisí, agenturou ENISA, dvěma provozovateli kořenových serverů DNS v EU a komunitou mnoha zúčastněných stran, aby vyhodnotila, jakou úlohu mají tito dva provozovatelé k zajišťování toho, aby internet zůstal globálně přístupný a neroztříštěný. VÍTÁ další diskusi o záměru Komise vytvořit alternativní evropskou službu pro přístup na globální internet (iniciativa DNS4EU) založenou na transparentním modelu, jenž bude odpovídat nejnovějšímu zabezpečení, ochraně dat a soukromí dané již samotným návrhem a obvyklým standardům a pravidlům, s cílem přispět ke zvýšení odolnosti a zároveň zachovat a zlepšit mezinárodní konektivitu všech členských států.

18. UZNÁVÁ, že je zapotřebí, aby Komise a členské státy společně usilovaly o rychlejší přijímání klíčových internetových standardů včetně IPv6 a zavedených standardů zabezpečení internetu, neboť napomáhají zvýšit celkovou úroveň bezpečnosti, odolnosti, otevřenosti a interoperability globálního internetu a zároveň zvyšují konkurenceschopnost průmyslu EU, a zejména provozovatelů internetové infrastruktury.

19. ZDŮRAZŇUJE význam koordinovaného přístupu i rozvoje a provádění účinných opatření na vnitrostátní úrovni, aby se posílila kybernetická bezpečnost sítí 5G. PODPORUJE přijetí dalších opatření v oblasti kybernetické bezpečnosti sítí 5G, jak je uvedeno v dodatku ke strategii kybernetické bezpečnosti EU a v návaznosti na výsledky zprávy o dopadech doporučení Komise o bezpečnosti sítí 5G, například pokud jde o definici dlouhodobého a komplexního přístupu k celému hodnotovému řetězci a ekosystému 5G. V zájmu dalšího posílení koordinovaného přístupu k bezpečnosti sítí 5G NALÉHAVĚ VYZÝVÁ členské státy, orgány EU a další příslušné zúčastněné strany, aby i nadále vyhodnocovaly pravidelně situaci, v rámci činnosti specializované skupiny pro spolupráci v oblasti bezpečnosti sítí a informací (NIS) si vyměňovaly informace a osvědčené postupy ohledně kybernetické bezpečnosti sítí 5G a pravidelně Radě předkládaly zprávy o dosaženém pokroku. Přestože poukazuje na odpovědnost členských států za ochranu vnitrostátní bezpečnosti, ZDŮRAZŇUJE, že je odhodlána využít soubor opatření EU pro kybernetickou bezpečnost sítí 5G a urychleně dokončit jeho zavedení a že i nadále bude usilovat o zajištění bezpečnosti sítí 5G a rozvoj budoucích generací sítí. Úzká spolupráce mezi členskými státy, Komisí a agenturou ENISA týkající se bezpečnosti sítí 5G by mohla být vzorem pro řešení dalších otázek v oblasti kybernetické bezpečnosti při současném respektování pravomocí členských států a zásad subsidiarity a proporcionality.

20. UZNÁVÁ význam dalšího začleňování kybernetické bezpečnosti do unijních mechanismů reakce na krize a jejich testování v rámci příslušných aktivit a ZDŮRAZŇUJE, že pro případ rozsáhlých a přeshraničních kybernetických incidentů a hrozeb je důležité posílit spolupráci a sdílení informací mezi jednotlivými kybernetickými komunitami v EU a propojit stávající iniciativy, struktury a postupy (jako jsou např. integrovaná opatření EU pro politickou reakci na krize (IPCR), síť týmů CSIRT, skupina NIS, Síť styčných organizací pro řešení kybernetických krizí (CyCLONe), Evropské centrum pro boj proti kyberkriminalitě, Zpravodajské a informační centrum EU (EU INTCEN) a další příslušné subjekty EU). S OHLEDEM NA pokrok, jehož bylo v této oblasti již dosaženo, OČEKÁVÁ návrh Komise týkající se procesu, milníků a harmonogramu pro vymezení společné kybernetické jednotky s cílem poskytnout přidanou hodnotu a jasné zaměření a zefektivnit unijní rámec pro řešení kybernetických bezpečnostních krizí, čehož lze mimo jiné dosáhnout připraveností, získáváním sdílených poznatků o situaci, zvyšováním koordinované odezvy a cvičení, a to transparentním a přírůstkovým způsobem, přičemž se zamezí zdvojování a překrývání a rovněž se budou respektovat pravomoci členských států.

21. ZDŮRAZŇUJE význam podporování spolupráce a výměny informací mezi příslušnými subjekty, jež se zabývají kybernetickou bezpečností, a příslušnými orgány v oblasti bezpečnosti a trestního soudnictví, např. donucovacími a soudními orgány, i potřebu rozšířit a zlepšit schopnost těchto orgánů vyšetřovat a stíhat kybernetickou kriminalitu a podporovat mezinárodní jednání a pravidla EU pro přeshraniční přístup k elektronickým důkazům. Bez ohledu na stávající technologické podmínky je nezbytné zachovat pravomoci příslušných orgánů v oblasti bezpečnosti a trestního soudnictví a zajistit jim zákonný přístup, jenž jim umožní plnit jejich úkoly, jak je stanoveno a povoleno právními předpisy. Tyto právní předpisy, které stanoví pravomoci v oblasti vymáhání práva, musí vždy plně dodržovat zásady spravedlivého procesu a další záruky, jakož i základní práva, zejména právo na respektování soukromého života a komunikace a právo na ochranu osobních údajů.

22. OPĚTOVNĚ POTVRZUJE, že podporuje rozvoj, provádění a používání silného šifrování jako nezbytného prostředku k ochraně základních práv a digitální bezpečnosti jednotlivců, vlád, průmyslu a společnosti, a současně UZNÁVÁ, že je třeba zajistit, aby příslušné orgány v oblasti bezpečnosti a trestního soudnictví, např. donucovací a justiční orgány, byly schopny vykonávat své zákonné pravomoci, a to online i offline, a chránily tak naše společnosti a občany. Příslušným orgánům musí být umožněn zákonný a cílený přístup k údajům, a to při plném dodržování základních práv a relevantních právních předpisů v oblasti ochrany údajů a při současném zachování kybernetické bezpečnosti. ZDŮRAZŇUJE, že jakákoliv přijatá opatření musí tyto zájmy pečlivě porovnat se zásadami nezbytnosti, proporcionality a subsidiarity.

23. POSILUJE a PROSAZUJE Budapešťskou úmluvu o počítačové kriminalitě a probíhající práci na Druhém dodatkovém protokolu k Budapešťské úmluvě. Navíc se i nadále podílí na mnohostranných výměnách informací v oblasti boje proti kybernetické kriminalitě, včetně procesů souvisejících s Radou Evropy, Úřadem OSN pro drogy a kriminalitu (UNODC) a Komisí OSN pro prevenci kriminality a trestní spravedlnost (CCPCJ), ve snaze posílit mezinárodní spolupráci v boji proti kybernetické kriminalitě, včetně výměny osvědčených postupů a technických poznatků a podpory budování kapacit, a současně dodržovat, prosazovat a chránit lidská práva a základní svobody.

24. Přestože národní bezpečnost zůstává výhradní odpovědností každého členského státu, UZNÁVÁ význam strategické zpravodajské spolupráce v oblasti kybernetických hrozeb a činností a VYZÝVÁ členské státy, aby prostřednictvím svých příslušných orgánů i nadále přispívaly k činnosti Zpravodajského a informačního centra EU (EU INTCEN) jakožto centra EU pro získávání poznatků o situaci a posuzování hrozeb v kybernetické oblasti a prozkoumaly návrh na možné zřízení pracovní skupiny členských států pro kybernetické zpravodajské informace s cílem posílit specializovanou kapacitu střediska INTCEN v této oblasti, a to na základě zpravodajských informací, které členské státy dobrovolně poskytnou, aniž by byly dotčeny jejich pravomoci.

25. ZDŮRAZŇUJE význam pevného a soudržného bezpečnostního rámce pro ochranu veškerého personálu, údajů, komunikačních sítí, informačních systémů a rozhodovacích procesů EU na základě komplexních, konzistentních a jednotných pravidel. Toho by se mělo dosáhnout zejména posílením odolnosti a zlepšením bezpečnostní kultury EU ve vztahu ke kybernetickým hrozbám a posílením bezpečnosti unijních sítí utajovaných a neutajovaných informací, přičemž se zároveň zajistí odpovídající správa a zpřístupní se dostatečné zdroje a schopnosti, a to i v souvislosti s posílením mandátu skupiny CERT-EU. V této souvislosti VÍTÁ probíhající jednání o zavedení společných pravidel pro bezpečnost informací, jež řádně zohlední bezpečnostní pravidla Rady pro ochranu utajovaných informací EU, jakož i vytvoření společných závazných pravidel pro kybernetickou bezpečnost pro všechny orgány, instituce a agentury EU.

26. V návaznosti na úsilí EU v oblasti kybernetické diplomacie se ZAVAZUJE, že zvýší efektivnost a účinnost souboru nástrojů pro diplomacii v oblasti kybernetiky, a se ZÁJMEM OČEKÁVÁ prohloubení diskuse o rozsahu a využití těchto nástrojů na základě poznatků, jež byly získány během dosavadního uplatňování. Tato jednání by měla přispět k prosazování bezpečnosti na mezinárodní úrovni, a to podporou dialogu a rozvojem společné vize v oblasti kybernetické bezpečnosti, posílením prevence, stability, spolupráce a dalším budováním důvěry a kapacit a případně použitím omezujících opatření, s cílem předcházet nepřátelským činnostem v kyberprostoru, jež se zaměřují na narušení integrity a bezpečnosti EU a jejích členských států, odrazovat od nich a reagovat na ně, což přispěje k mezinárodní bezpečnosti a stabilitě a upevní pozici EU v kybernetické oblasti, a to za plného respektování vnitrostátních pravomocí a výsad. Zvláštní pozornost by se měla věnovat zejména předcházení kybernetickým útokům se systémovými účinky, které by mohly mít dopad na naše dodavatelské řetězce, kritickou infrastrukturu a základní služby, demokratické instituce a procesy a narušit naši hospodářskou bezpečnost, včetně kybernetických krádeží duševního vlastnictví, ale i obraně před takovými útoky. Členské státy a orgány EU by dále rovněž měly uvažovat nad pojítkem mezi unijním rámcem pro řešení kybernetických bezpečnostních krizí, souborem nástrojů pro diplomacii v oblasti kybernetiky a ustanoveními čl. 42 odst. 7 SEU a článku 222 SFEU, zejména prostřednictvím práce založené na scénářích, aby vybudovaly společné chápání praktických postupů pro provádění čl. 42 odst. 7 SEU.

27. UZNÁVÁ, že je důležité posílit spolupráci s mezinárodními organizacemi a partnerskými zeměmi, aby se pokročilo ve společném chápání problematiky kybernetických hrozeb, rozvíjely se dialogy a mechanismy spolupráce, případně se identifikovaly diplomatické reakce založené na spolupráci a zlepšilo se sdílení informací, a to i prostřednictvím vzdělávání, odborné přípravy a cvičení. Především ZDŮRAZŇUJE, že silné transatlantické partnerství v oblasti kybernetické bezpečnosti přispívá k naší společné bezpečnosti, stabilitě a prosperitě, a BERE NA VĚDOMÍ ustanovení o spolupráci v oblasti kybernetické bezpečnosti v rámci dohody o obchodu a spolupráci mezi EU a Spojeným královstvím. PŘIPOMÍNAJÍC klíčové úspěchy spolupráce mezi EU a NATO v oblasti kybernetické bezpečnosti, kterých se dosáhlo během provádění varšavského společného prohlášení z roku 2016 a bruselského společné prohlášení z roku 2018, opětovně zdůrazňuje význam zkvalitněné, vzájemně posilující a prospěšné spolupráce prostřednictvím vzdělávání, odborné přípravy, cvičení a koordinované reakce na nepřátelské činnosti v kyberprostoru, a to na základě zásad transparentnosti, reciprocity, inkluzivnosti a při plném respektování rozhodovací samostatnosti a postupů obou organizací.

28. S cílem přispět ke globálnímu, otevřenému, svobodnému, stabilnímu a bezpečnému kyberprostoru, jehož význam pro pokračující prosperitu, růst, bezpečnost, dobré životní podmínky, konektivitu a integritu našich společností neustále roste, SE ZAVAZUJE k tomu, že bude neustále zapojena do procesů vytváření norem v mezinárodních organizacích, zejména do procesů souvisejících s prvním výborem OSN, že bude prosazovat a podílet se na uznání toho, že je v kyberprostoru zapotřebí uplatňovat mezinárodní právo a dodržovat normy, pravidla a zásady odpovědného chování státu v kyberprostoru, a to i podporou rychlého zavedení akčního programu na prosazování odpovědného chování států v kybernetickém prostoru, což představuje konstruktivní, inkluzivní a konsenzuální činnosti navazující na stávající procesy skupin vládních expertů i otevřených pracovních skupin.

29. PŘIPOMÍNÁ, že se pevně zavázala k účinnému multilateralismu a světovému pořádku založenému na pravidlech, jehož jádro tvoří OSN, a je odhodlána posílit spolupráci a koordinaci s mezinárodními a regionálními organizacemi, jako jsou systém OSN, NATO, Rada Evropy, OBSE, OECD, Africká unie, Organizace amerických států (OAS), Sdružení národů jihovýchodní Asie (ASEAN), regionální fórum ASEAN (ARF), Rada pro spolupráci v Zálivu (GCC) a Liga arabských států (LAS), pokud jde o diskuse o záležitostech z kybernetické oblasti, jakož i o pokračování a rozšiřování strukturovaných dialogů a konzultací EU se třetími zeměmi o otázkách kybernetické bezpečnosti. ZDŮRAZŇUJE svou aktivní podporu OSN, zejména ve vztahu k její Agendě 2030, včetně cílů udržitelného rozvoje, a VÍTÁ plán generálního tajemníka OSN pro spolupráci v digitální oblasti, jakož i generálním tajemníkem OSN vypracovaný program pro odzbrojení, jež posilují odpovědnost a dodržování norem v kyberprostoru a přispívají k předcházení a mírovému řešení sporů pramenících z nepřátelské činnosti v kyberprostoru. VÍTÁ návrh vysokého představitele pro zahraniční věci a bezpečnostní politiku zřídit neformální síť EU pro kybernetickou diplomacii, jež by podpořila zapojení EU i členských států do mezinárodních kybernetických otázek a prohloubila jejich odborné znalosti v této oblasti za účelem posílení koordinované osvětové činnosti.

30. Se ZÁJMEM OČEKÁVÁ nadcházející návrh přezkumu politického rámce EU pro kybernetickou obranu (CDFP) a ZAVAZUJE SE, že bude i nadále usilovat o zdůrazňování aspektů kybernetické bezpečnosti a kybernetické obrany s cílem zajistit, aby byly plně začleněny do širší oblasti bezpečnosti a obrany, zejména v souvislosti s prací na Strategickém kompasu. DOMNÍVÁ SE, že k rozvoji těchto diskusí přispěje připravovaná „Vojenská vize a strategie pro kyberprostor jako oblast operací“. VÍTÁ iniciativu Evropské obranné agentury (EDA) na posílení spolupráce mezi vojenskými skupinami pro reakci na počítačové hrozby (CERT) a PODPORUJE úsilí, jež bylo vynaloženo na zlepšení civilně-vojenských synergií a koordinaci v oblasti kybernetické obrany, kybernetické bezpečnosti a aspektů souvisejících s vesmírem, a to i prostřednictvím specializovaných projektů stálé strukturované spolupráce (PESCO).

31. VÍTÁ návrh na vypracování agendy EU pro budování vnějších kybernetických kapacit, návrh na vytvoření Rady EU pro budování kybernetických kapacit a zřízení a zavedení sítě EU CyberNet (síť EU pro budování kybernetických kapacit), aby se posílila kybernetická odolnost a kybernetické kapacity na celosvětové úrovni. V této souvislosti VÍTÁ spolupráci s členskými státy i s partnery z veřejného a soukromého sektoru, především se světovým fórem pro počítačovou odbornost (Global Forum on Cyber Expertise, GFCE) a s dalšími příslušnými mezinárodními subjekty, s cílem zajistit koordinaci a zabránit zdvojování činností. Především PODPORUJE spolupráci s partnery ze západního Balkánu a ze zemí východního a jižního sousedství EU.

32. K zajištění toho, aby všechny země byly schopny těžit ze sociálních, hospodářských a politických přínosů internetu a využívání technologií, SE ZAVAZUJE, že bude partnerským zemím pomáhat při řešení stále většího problému, jímž je nepřátelská činnost v kyberprostoru, a to zejména činnost narušující rozvoj hospodářství a společnosti, jakož i integritu a bezpečnost demokratických systémů, přičemž toto úsilí bude rovněž vycházet z Evropského akčního plánu pro demokracii.

33. S cílem zajistit vypracování, provádění a sledování návrhů předložených v rámci strategie kybernetické bezpečnosti EU a s ohledem na víceletý charakter některých iniciativ VYZÝVÁ Komisi a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku, aby vypracovali podrobný prováděcí plán, jenž určí priority a harmonogram plánovaných opatření. Bude SLEDOVAT pokrok, jehož se při provádění těchto závěrů prostřednictvím akčního plánu dosáhlo, přičemž v úzké spolupráci s Evropskou komisí a vysokým představitelem bude Rada tento plán pravidelně přezkoumávat a aktualizovat.