Rada
Európskej únie

V Bruseli 23. marca 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	22. marca 2021
Komu:	Delegácie
Predmet:	Závery Rady o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu – závery Rady, ktoré Rada schválila na svojom zasadnutí 22. marca 2021

Delegáciám v prílohe zasielame závery Rady o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu, ktoré Rada schválila na svojom zasadnutí 22. marca 2021.

PRÍLOHA

Závery Rady o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu

RADA EURÓPSKEJ ÚNIE,

PRIPOMÍNAJÚC svoje závery o:

– spoločnom oznámení Európskemu parlamentu a Rade z 25. júna 2013 s názvom Stratégia kybernetickej bezpečnosti Európskej únie: otvorený, bezpečný a chránený kybernetický priestor[1],

– správe internetu[2],

– spoločnom oznámení Európskemu parlamentu a Rade z 20. novembra 2017: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ[3],

– budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ[4],

– význame 5G pre európske hospodárstvo a potrebe zmierniť bezpečnostné riziká spojené s 5G[5],

– budúcnosti vysoko digitalizovanej Európy po roku 2020: „Zvýšenie digitálnej a hospodárskej konkurencieschopnosti v celej Únii a digitálna súdržnosť“[6],

– komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám[7],

– formovaní digitálnej budúcnosti Európy[8],

---

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

– digitálnej diplomacii[9],

– posilnení odolnosti a boji proti hybridným hrozbám vrátane dezinformácií v súvislosti s pandémiou COVID-19[10],

– kybernetickej diplomacii[11],

– koordinovanej reakcii EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu[12],

– rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“), 19. júna 2017[13],

– usmerneniach EÚ týkajúcich sa budovania vonkajších kybernetických kapacít[14],

– obnove, ktorá urýchľuje prechod na dynamickejší, odolnejší a konkurencieschopnejší európsky priemysel[15],

– kybernetickej bezpečnosti pripojených zariadení[16],

– posilnení európskeho systému kybernetickej odolnosti a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti[17],

– a závery Rady o šifrovaní – bezpečnosť prostredníctvom šifrovania a bezpečnosť napriek šifrovaniu[18],

---

9 12804/20.
10 14064/20.
11 6122/15 + COR 1.
12 10086/18.
13 10474/17.
14 10496/18.
15 13004/20.
16 13629/20.
17 14540/16.
18 13084/1/20 REV 1.

– a vyhlásenie členských štátov z 15. októbra 2020 o budovaní cloudu budúcej generácie pre podniky a verejný sektor v EÚ,

PRIPOMÍNAJÚC závery Európskej rady o pandémii COVID-19, jednotnom trhu, priemyselnej politike, digitálnej oblasti a vonkajších vzťahoch z 1. – 2. októbra 2020[19], ako aj závery o dezinformáciách a hybridných hrozbách a o novom strategickom programe na roky 2019 – 2024 z 20. júna 2019[20],

PRIPOMÍNAJÚC Globálnu stratégiu pre zahraničnú a bezpečnostnú politiku Európskej únie – „Spoločná vízia, spoločný postup: silnejšia Európa“ z 28. júna 2016,

PRIPOMÍNAJÚC oznámenie Európskej komisie o formovaní digitálnej budúcnosti Európy z 19. decembra 2020[21] a o stratégii EÚ pre bezpečnostnú úniu z 24. júla 2020[22],

PRIPOMÍNAJÚC spoločné oznámenie Európskej komisie a vysokého predstaviteľa o novej agende EÚ – USA pre globálnu zmenu z 2. decembra 2020[23],

1. ZDÔRAZŇUJE skutočnosť, že kybernetická bezpečnosť má zásadný význam pre budovanie odolnej, zelenej a digitálnej Európy, a VÍTA spoločné oznámenie Európskemu parlamentu a Rade s názvom Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde, v ktorom sa načrtáva nový rámec činnosti EÚ v oblasti odolnosti, technologickej suverenity a líderstva, ako aj ochrany jej obyvateľov, podnikov a inštitúcií pred kybernetickými incidentmi a hrozbami a zároveň na posilnenie dôvery jednotlivcov a organizácií v schopnosť EÚ podporovať bezpečné a spoľahlivé siete a informačné systémy, infraštruktúru a konektivitu, ako aj propagovať a chrániť globálny, otvorený, slobodný, stabilný a bezpečný kybernetický priestor založený na ľudských právach, základných slobodách, demokracii a právnom štáte.

---

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

2. UZNÁVA, že pandémia COVID-19 presunula zvýšenú potrebu dôvery v nástroje a systémy informačných a komunikačných technológií (IKT) a ich bezpečnosť do popredia nášho každodenného života. ZDÔRAZŇUJE, že kybernetická bezpečnosť a globálny a otvorený internet majú zásadný význam pre fungovanie verejnej správy a inštitúcií na vnútroštátnej úrovni aj na úrovni EÚ, ako aj pre našu spoločnosť a hospodárstvo ako celok.

3. ZDÔRAZŇUJE, že je potrebné zvýšiť informovanosť o kybernetických otázkach na politickej a strategickej úrovni rozhodovania tým, že sa rozhodovacím orgánom poskytnú príslušné znalosti a informácie, a ZDÔRAZŇUJE, že je potrebné zvýšiť informovanosť širokej verejnosti a podporovať kybernetickú hygienu.

4. VYZÝVA NA presadzovanie a ochranu základných hodnôt EÚ, ktorými sú demokracia, právny štát, ľudské práva a základné slobody vrátane práva na slobodu prejavu a práva na informácie, práva na slobodu zhromažďovania a združovania a práva na súkromie v kybernetickom priestore. V tejto súvislosti VÍTA ďalšie nepretržité úsilie o ochranu obhajcov ľudských práv, zástupcov občianskej spoločnosti a akademickej obce, ktorí sa zaoberajú otázkami kybernetickej bezpečnosti, ochrany údajov, sledovania a cenzúry online, a to poskytovaním ďalších praktických usmernení, presadzovaním najlepších postupov a zintenzívnením úsilia EÚ o predchádzanie porušovaniu a zneužívaniu ľudských práv a zneužívaniu nových technológií, v prípade potreby najmä diplomatickými opatreniami, ako aj kontrolou vývozu takýchto technológií. V tejto súvislosti ZDÔRAZŇUJE význam akčného plánu EÚ pre ľudské práva a demokraciu na roky 2020 – 2024 a jej usmernení v oblasti ľudských práv týkajúcich sa slobody prejavu online a offline.

5. ZDÔRAZŇUJE, že dosiahnutie strategickej autonómie pri zachovaní otvoreného hospodárstva je kľúčovým cieľom Únie na to, aby mohla samostatne určovať svoje hospodárske smerovanie a záujmy. To zahŕňa posilnenie schopnosti prijímať autonómne rozhodnutia v oblasti kybernetickej bezpečnosti s cieľom posilniť vedúce postavenie EÚ v digitálnej oblasti a jej strategické kapacity. PRIPOMÍNA, že to zahŕňa aj identifikáciu a zníženie strategických závislostí a zvýšenie odolnosti v najcitlivejších priemyselných ekosystémoch a konkrétnych oblastiach. ZDÔRAZŇUJE, že to môže zahŕňať aj diverzifikáciu výrobných a dodávateľských reťazcov, posilnenie a lákanie investícií a výroby v Európe, skúmanie alternatívnych riešení a obehových modelov a podporu širokej priemyselnej spolupráce medzi členskými štátmi.

6. Vzhľadom na nedostatok digitálnych a kybernetickobezpečnostných zručností pracovnej sily ZDÔRAZŇUJE, že je dôležité uspokojiť dopyt po vyškolenej pracovnej sile v oblasti digitálnych technológií a kybernetickej bezpečnosti, a to najmä rozvíjaním, udržaním a prilákaním najlepších talentov, napríklad prostredníctvom vzdelávania a odbornej prípravy, aby bolo možné digitalizovať našu spoločnosť spôsobom, ktorý je bezpečný z kybernetického hľadiska. PODPORUJE väčšie zapojenie žien a dievčat do vzdelávania v oblasti vedy, technológií, inžinierstva, matematiky (STEM) a do zvyšovania úrovne digitálnych zručností alebo ich získavania v rámci pracovných miest v oblasti IKT ako jedného z prostriedkov na preklenutie rodovej digitálnej priepasti.

7. PRIPOMÍNA, že spoločný a komplexný prístup EÚ ku kybernetickej diplomacii je zameraný na prispievanie k predchádzaniu konfliktom, zmierňovaniu kybernetických hrozieb a väčšej stabilite v medzinárodných vzťahoch. V tejto súvislosti OPÄTOVNE POTVRDZUJE svoj záväzok urovnávať medzinárodné spory v kybernetickom priestore mierovými prostriedkami, a že všetko diplomatické úsilie EÚ by sa malo prioritne zamerať na podporu bezpečnosti a stability v kybernetickom priestore prostredníctvom posilnenej medzinárodnej spolupráce a na zníženie rizika mylného vnímania situácií, ich eskalácie a konfliktov, ktoré môžu prameniť z incidentov v oblasti IKT, a PODPORUJE ďalší rozvoj a sfunkčnenie opatrení na budovanie dôvery na regionálnej a medzinárodnej úrovni. OPAKUJE výzvu Valného zhromaždenia Organizácie Spojených národov odsúhlasenú konsenzom, aby sa členské štáty OSN pri využívaní IKT riadili odporúčaniami zo správ skupiny vládnych expertov, a OPÄTOVNE POTVRDZUJE uplatňovanie medzinárodného práva, najmä Charty OSN v celom jej rozsahu, v kybernetickom priestore.

8. OPÄTOVNE POTVRDZUJE, že v záujme zásadného formovania medzinárodných noriem a štandardov v oblasti vznikajúcich technológií a technickej a logickej infraštruktúry, ktorá je nevyhnutná pre všeobecnú dostupnosť a integritu verejného jadra internetu, aby boli tieto normy a štandardy v súlade so všeobecnými hodnotami a hodnotami EÚ, je v Únii nevyhnutný ich ďalší rozvoj prostredníctvom prístupu viacerých zainteresovaných strán. Tým sa zabezpečí, že internet zostane globálny, otvorený, slobodný, stabilný a bezpečný, že používanie a rozvoj digitálnych technológií bude rešpektovať ľudské práva a že ich používanie bude zákonné, bezpečné a etické. Berie NA VEDOMIE nadchádzajúcu stratégiu normalizácie a ZAVÄZUJE SA k proaktívnej a koordinovanej osvetovej činnosti na podporu vedúceho postavenia EÚ a cieľov EÚ na medzinárodnej úrovni, a to aj v rámci rôznych medzinárodných normalizačných orgánov a spoluprácou s podobne zmýšľajúcimi partnermi, občianskou spoločnosťou, akademickou obcou a súkromným sektorom.

9. DÔRAZNE PODPORUJE model správy internetu a kybernetickej bezpečnosti, ktorý pozostáva z viacerých zainteresovaných strán a zaväzuje sa k posilneniu pravidelných a štruktúrovaných výmen so zainteresovanými stranami vrátane súkromného sektora, akademickej obce a občianskej spoločnosti na medzinárodných fórach, a to aj v kontexte parížskej výzvy na dôveryhodnosť a bezpečnosť kybernetického priestoru. PODPORUJE univerzálny, cenovo dostupný a rovnaký prístup k internetu, ktorý preklenie digitálnu priepasť, a najmä posilnenie postavenia žien a dievčat a ľudí v zraniteľných alebo marginalizovaných situáciách, a to pri tvorbe politík, ako aj pri používaní internetu.

10. ZDÔRAZŇUJE potrebu začleniť v nadchádzajúcich rokoch kybernetickú bezpečnosť do digitálnych investícií a iniciatív a postupne prispievať k vytvoreniu rovnakých podmienok v oblasti kybernetickej bezpečnosti a BERIE NA VEDOMIE plán Komisie zvýšiť verejné výdavky a využiť efekt finančnej páky súkromných investícií v oblasti kybernetickej bezpečnosti. ZDÔRAZŇUJE význam malých a stredných podnikov (MSP) v ekosystéme kybernetickej bezpečnosti a UZNÁVA príslušné finančné nástroje, ktoré sú k dispozícii na podporu silného zamerania sa na kybernetickú bezpečnosť v medziach digitálnej transformácie počas viacročného finančného rámca (VFR) v rokoch 2021 – 2027, ako aj v rámci Mechanizmu na podporu obnovy a odolnosti.

11. So ZÁUJMOM OČAKÁVA urýchlené vykonávanie nariadenia o Európskom centre priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieti národných koordinačných centier (CCCN) vrátane rýchleho zriadenia a sprevádzkovania Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti v Bukurešti. Rýchle prijatie jeho programu prispeje k maximalizácii účinkov investícií s cieľom posilniť vedúce postavenie Únie a strategickú autonómiu v oblasti kybernetickej bezpečnosti, podporiť technologické kapacity a zručnosti a zvýšiť globálnu konkurencieschopnosť Únie prostredníctvom vstupov od priemyselných a akademických komunít v oblasti kybernetickej bezpečnosti vrátane MSP a výskumných centier, ktoré budú ťažiť zo systematickejšej, inkluzívnejšej a strategickejšej spolupráce so zreteľom na súdržnosť Únie a všetkých jej členských štátov.

12. VÍTA prebiehajúcu prácu pod vedením agentúry ENISA spolu s členskými štátmi a zainteresovanými stranami s cieľom poskytnúť EÚ systémy certifikácie produktov, služieb a procesov IKT, ktoré by mali prispieť k zvýšeniu celkovej úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. V tejto súvislosti SO ZÁUJMOM OČAKÁVA priebežný pracovný program Únie s cieľom vytvoriť systémy certifikácie kybernetickej bezpečnosti EÚ v rámci aktu o kybernetickej bezpečnosti. V tejto súvislosti UZNÁVA kľúčovú úlohu EÚ pri vypracúvaní noriem, ktoré môžu formovať kybernetickobezpečnostné prostredie, a prispievajú k zabezpečeniu spravodlivej hospodárskej súťaže v EÚ a na celosvetovej úrovni, podporujú prístup na trh, ako aj riešenie bezpečnostných rizík pri súčasnom zabezpečení uplatniteľnosti legislatívneho rámca EÚ.

13. OPAKUJE, že je z dlhodobého hľadiska dôležité posúdiť potrebu horizontálnych právnych predpisov, ktorými by sa ustanovili okrem iného potrebné podmienky prístupu na trh, s cieľom riešiť všetky relevantné aspekty kybernetickej bezpečnosti pripojených zariadení, ako je dostupnosť, integrita a dôvernosť. V tejto súvislosti VÍTA diskusiu o preskúmaní rozsahu pôsobnosti takýchto právnych predpisov a ich prepojenia s rámcom certifikácie kybernetickej bezpečnosti vymedzeným v akte o kybernetickej bezpečnosti s cieľom zvýšiť úroveň bezpečnosti na digitálnom jednotnom trhu. ZDÔRAZŇUJE, že požiadavky na kybernetickú bezpečnosť by sa mali vymedziť v súlade s príslušnými právnymi predpismi Únie, okrem iného v akte o kybernetickej bezpečnosti, novom legislatívnom rámci, nariadení o európskej normalizácii a v prípadných budúcich horizontálnych právnych predpisoch, aby sa predišlo nejasnostiam a fragmentácii v právnych predpisoch.

14. UZNÁVA význam komplexného a horizontálneho prístupu ku kybernetickej bezpečnosti v Únii pri plnom rešpektovaní právomocí a potrieb členských štátov, ako aj význam neustálej podpory technickej pomoci a spolupráce pri budovaní kapacít členských štátov. Vzhľadom na vývoj situácie v oblasti kybernetických hrozieb BERIE NA VEDOMIE nový návrh smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorý vychádza zo smernice NIS, a opätovne potvrdzuje svoju podporu posilneniu a harmonizácii vnútroštátnych rámcov kybernetickej bezpečnosti a trvalej spolupráce medzi členskými štátmi. Okrem toho ZDÔRAZŇUJE potrebu zosúladenia a súdržnosti sektorových právnych predpisov v tejto oblasti.

15. Berie NA VEDOMIE návrh Komisie na podporu členských štátov pri zriaďovaní a posilňovaní stredísk bezpečnostných operácií s cieľom vybudovať ich sieť SOC v celej EÚ a ďalej monitorovať a predvídať signály možnosti útokov na siete. V tejto súvislosti OČAKÁVA podrobné plány Komisie týkajúce sa siete stredísk bezpečnostných operácií pri súčasnom rešpektovaní právomoci členských štátov. PRIPOMÍNA úsilie členských štátov s podporou EÚ zriadiť sektorové, celoštátne a regionálne jednotky CSIRT a národné alebo európske strediská pre výmenu a analýzu informácií ako súčasť efektívnej siete partnerstiev v oblasti kybernetickej bezpečnosti v Únii. So ZÁUJMOM OČAKÁVA preskúmanie potenciálu tejto siete z hľadiska posilnenia stredísk bezpečnostných operácií, ako aj ich doplnkovosti a koordinácie s existujúcimi sieťami a aktérmi (najmä sieťou jednotiek CSIRT) s cieľom podporiť efektívnu, bezpečnú a spoľahlivú kultúru výmeny informácií. ZDÔRAZŇUJE, že tento proces bude vychádzať z práce vykonanej v súvislosti s iniciatívami v oblasti umelej inteligencie a vysokovýkonnej výpočtovej techniky a práce európskych centier digitálnych inovácií.

16. Berie NA VEDOMIE možný vývoj bezpečného systému konektivity, ktorý vychádza z európskej kvantovej komunikačnej infraštruktúry (EuroQCI) a vládnej satelitnej komunikácie Európskej únie (GOVSATCOM), a UZNÁVA, že akýkoľvek prípadný budúci vývoj by mal byť založený na robustnom rámci kybernetickej bezpečnosti a mal by zohľadňovať celú infraštruktúru elektronických komunikácií, ako sú kozmické, pozemné a podmorské sieťové systémy.

17. So ZÁUJMOM OČAKÁVA diskusie s Komisiou, agentúrou ENISA, dvoma prevádzkovateľmi koreňových DNS serverov EÚ a komunitou viacerých zainteresovaných strán s cieľom posúdiť úlohu prevádzkovateľov uvedených serverov, pokiaľ ide o zaručenie toho, aby internet zostal celosvetovo dostupný a nefragmentovaný. VÍTA ďalšiu diskusiu o zámere Komisie vytvoriť alternatívnu európsku službu pre prístup ku globálnemu internetu (iniciatíva „DNS4EU“) založenú na transparentnom modeli, ktorý bude v súlade s najnovšími normami a pravidlami v oblasti bezpečnosti, ochrany údajov a ochrany súkromia už v štádiu návrhu a ako štandard, s cieľom prispieť k zvýšeniu odolnosti a zároveň zachovať a posilniť medzinárodnú konektivitu pre všetky členské štáty.

18. UZNÁVA potrebu spoločného úsilia Komisie a členských štátov o urýchlenie zavádzania kľúčových internetových noriem vrátane IPv6 a zavedených noriem v oblasti bezpečnosti internetu, keďže zásadne pomáhajú zvyšovať celkovú úroveň bezpečnosti, odolnosti, otvorenosti a interoperability globálneho internetu a zároveň zvyšujú konkurencieschopnosť priemyslu EÚ, a najmä prevádzkovateľov internetovej infraštruktúry.

19. ZDÔRAZŇUJE význam koordinovaného prístupu, ako aj vypracovania a vykonávania účinných opatrení na vnútroštátnej úrovni na posilnenie kybernetickej bezpečnosti sietí 5G. PODPORUJE ďalšie kroky, ktoré sa majú prijať v oblasti kybernetickej bezpečnosti sietí 5G, ako sa uvádza v dodatku k stratégii kybernetickej bezpečnosti EÚ a ktoré vychádzajú z výsledkov správy o vplyve odporúčania Komisie na bezpečnosť sietí 5G, napríklad pokiaľ ide o vymedzenie dlhodobého a komplexného prístupu zameraného na celý hodnotový reťazec a ekosystém 5G. S cieľom ďalej posilniť koordinovaný prístup k bezpečnosti sietí 5G NALIEHAVO VYZÝVA členské štáty, inštitúcie EÚ a iné príslušné zainteresované strany, aby pokračovali vo svojom pravidelnom hodnotení a vymieňali si informácie a najlepšie postupy v rámci práce osobitnej skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zameranej na kybernetickú bezpečnosť 5G a pravidelne podávali Rade správy o dosiahnutom pokroku. Hoci podčiarkuje zodpovednosť členských štátov za ochranu národnej bezpečnosti, ZDÔRAZŇUJE svoje pevné odhodlanie uplatňovať a urýchlene dokončiť vykonávanie opatrení súboru nástrojov EÚ pre 5G a pokračovať v úsilí o zaručenie bezpečnosti sietí 5G a rozvoja budúcich generácií sietí. Úzka spolupráca medzi členskými štátmi, Komisiou a agentúrou ENISA v oblasti bezpečnosti sietí 5G by mohla slúžiť ako príklad pre iné otázky v oblasti kybernetickej bezpečnosti pri rešpektovaní právomocí členských štátov a zásad subsidiarity a proporcionality.

20. UZNÁVA význam hlbšej integrácie kybernetickej bezpečnosti do mechanizmov reakcie EÚ na krízy a ich testovania v príslušných cvičeniach a ZDÔRAZŇUJE význam posilnenia spolupráce a výmeny informácií medzi rôznymi kybernetickými komunitami v EÚ a prepojenia existujúcich iniciatív, štruktúr a postupov (ako sú IPCR, sieť jednotiek CSIRT, skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieť styčných organizácií pre kybernetické krízy CyCLONe, Európske centrum boja proti počítačovej kriminalite, EU INTCEN a iné príslušné orgány EÚ) v prípade rozsiahlych a cezhraničných kybernetických hrozieb a incidentov. BERÚC DO ÚVAHY pokrok, ktorý sa už v tejto oblasti dosiahol, OČAKÁVA návrh Komisie týkajúci sa procesu, čiastkových cieľov a harmonogramu vymedzenia spoločnej kybernetickej jednotky s cieľom vytvoriť pridanú hodnotu a dosiahnuť jasné zameranie a zefektívnenie rámca krízového riadenia kybernetickej bezpečnosti EÚ, a to aj prostredníctvom pripravenosti, spoločného situačného povedomia, posilnenia koordinovanej reakcie a cvičení, a to transparentným a prírastkovým spôsobom, pričom sa zabráni duplicite a prekrývaniu a zároveň sa dodržia právomoci členských štátov.

21. ZDÔRAZŇUJE význam podpory spolupráce a výmeny informácií medzi príslušnými aktérmi v oblasti kybernetickej bezpečnosti a príslušnými orgánmi v oblasti bezpečnosti a trestnej justície, napr. orgánmi presadzovania práva a justičnými orgánmi, ako aj potrebu rozšíriť a zlepšiť kapacitu týchto orgánov vyšetrovať a stíhať počítačovú kriminalitu a podporovať medzinárodné rokovania a pravidlá EÚ týkajúce sa cezhraničného prístupu k elektronickým dôkazom. Nezávisle od aktuálneho technologického prostredia je nevyhnutné zachovať právomoci príslušných orgánov v oblasti bezpečnosti a trestnej justície prostredníctvom zákonného prístupu na účely plnenia ich úloh, ako je stanovené a povolené zákonom. Takéto zákony, ktoré ustanovujú právomoci na presadzovanie práva, musia vždy v plnej miere rešpektovať riadny proces a iné záruky, ako aj základné práva, najmä právo na rešpektovanie súkromného života a komunikácií a právo na ochranu osobných údajov.

22. OPÄTOVNE POTVRDZUJE svoju podporu vývoju, implementácii a používaniu silného šifrovania ako nevyhnutného prostriedku na ochranu základných práv a digitálnej bezpečnosti jednotlivcov, vlád, priemyslu a spoločnosti a zároveň UZNÁVA potrebu zabezpečiť schopnosť príslušných orgánov v oblasti bezpečnosti a trestnej justície, napr. orgánov presadzovania práva a justičných orgánov, vykonávať svoje zákonné právomoci, a to online aj offline, s cieľom chrániť naše spoločnosti a občanov. Príslušné orgány musia mať prístup k údajom zákonným a cieleným spôsobom pri plnom dodržiavaní základných práv a príslušných právnych predpisov o ochrane údajov a súčasne dbať na kybernetickú bezpečnosť. ZDÔRAZŇUJE, že pri všetkých prijatých opatreniach sa musí starostlivo zaistiť rovnováha medzi uvedenými záujmami a zásadami nevyhnutnosti, proporcionality a subsidiarity.

23. PODPORUJE a PROPAGUJE budapeštiansky Dohovor o počítačovej kriminalite a prácu, ktoré prebieha na druhom dodatkovom protokole k nemu. Okrem toho sa naďalej zapája do mnohostranných výmen v oblasti počítačovej kriminality, a to aj v rámci procesov súvisiacich s Radou Európy, Úradom OSN pre drogy a kriminalitu (UNODC) a Komisiou pre prevenciu kriminality a trestnú justíciu (CCPCJ), s cieľom zabezpečiť posilnenú medzinárodnú spoluprácu v boji proti počítačovej kriminalite vrátane výmeny najlepších postupov a technických poznatkov a podporovať budovanie kapacít pri súčasnom dodržiavaní, presadzovaní a ochrane ľudských práv a základných slobôd.

24. Hoci národná bezpečnosť zostáva vo výlučnej zodpovednosti každého členského štátu, UZNÁVA význam strategickej spravodajskej spolupráce v oblasti kybernetických hrozieb a kybernetických činností a VYZÝVA členské štáty, aby prostredníctvom svojich príslušných orgánov naďalej prispievali k práci centra EU INTCEN ako centra pre situačné povedomie a posudzovanie hrozieb v kybernetických otázkach pre EÚ a aby preskúmali návrh o možnom zriadení pracovnej skupiny členských štátov pre kybernetickú spravodajskú službu s cieľom posilniť osobitné kapacity INTCEN v tejto oblasti, a to na základe dobrovoľných spravodajských príspevkov členských štátov bez toho, aby boli dotknuté ich právomoci.

25. ZDÔRAZŇUJE význam robustného a konzistentného bezpečnostného rámca založeného na komplexných, konzistentných a homogénnych pravidlách slúžiaceho na ochranu všetkých zamestnancov EÚ a jej údajov, komunikačných sietí a informačných systémov a rozhodovacích procesov. To by sa malo dosiahnuť najmä posilnením odolnosti a zlepšením bezpečnostnej kultúry EÚ v boji proti kybernetickým hrozbám a posilnením bezpečnosti utajovaných a neutajovaných sietí EÚ pri súčasnom zabezpečení primeranej správy a sprístupnenia dostatočných zdrojov a spôsobilostí, a to aj v kontexte posilnenia mandátu tímu CERT-EU. V tejto súvislosti VÍTA prebiehajúce diskusie o vytvorení spoločných pravidiel bezpečnosti informácií s náležitým ohľadom na bezpečnostné predpisy Rady na ochranu utajovaných skutočností EÚ, ako aj vymedzenie spoločných záväzných pravidiel kybernetickej bezpečnosti pre všetky inštitúcie, orgány a agentúry EÚ.

26. VYCHÁDZAJÚC z úsilia EÚ v oblasti kybernetickej diplomacie sa ZAVÄZUJE zvýšiť účinnosť a efektívnosť súboru nástrojov kybernetickej diplomacie a SO ZÁUJMOM OČAKÁVA prehĺbenie diskusií o jeho rozsahu pôsobnosti a využití na základe doterajších skúseností z uplatňovania tohto nástroja. Tieto diskusie by mali prispieť k podpore bezpečnosti na medzinárodnej úrovni prostredníctvom podpory dialógu a spoločnej vízie, pokiaľ ide o záležitosti kybernetickej bezpečnosti, posilňovaním prevencie, stability, spolupráce, posilňovania dôvery a budovania kapacít a v prípade potreby uplatňovania reštriktívnych opatrení s cieľom predchádzať škodlivým kybernetickým činnostiam zameraným na integritu a bezpečnosť EÚ a jej členských štátov, odrádzať od nich a reagovať na ne, a tým prispievať k medzinárodnej bezpečnosti a stabilite a konsolidovať prístup EÚ ku kybernetickej bezpečnosti pri plnom rešpektovaní vnútroštátnych právomocí a výsad. Osobitná pozornosť by sa mala venovať najmä predchádzaniu a boju proti kybernetickým útokom so systémovými účinkami, ktoré by mohli mať vplyv na naše dodávateľské reťazce, kritickú infraštruktúru a základné služby, demokratické inštitúcie a procesy a ktoré by mohli ohroziť našu hospodársku bezpečnosť vrátane krádeže duševného vlastníctva umožnenej kybernetickými technológiami. Členské štáty a inštitúcie EÚ by mali tiež ďalej uvažovať o prepojení medzi rámcom krízového riadenia kybernetickej bezpečnosti EÚ, súborom nástrojov kybernetickej diplomacie a ustanoveniami článku 42 ods. 7 ZEÚ a článku 222 ZFEÚ, najmä prostredníctvom práce založenej na scenároch s cieľom dosiahnuť spoločné chápanie praktických spôsobov vykonávania článku 42 ods. 7 ZEÚ.

27. UZNÁVA význam posilnenia spolupráce s medzinárodnými organizáciami a partnerskými krajinami s cieľom dosiahnuť pokrok v spoločnom chápaní situácie v oblasti kybernetických hrozieb, rozvíjať dialógy a mechanizmy spolupráce, v prípade potreby identifikovať kooperatívne diplomatické reakcie, ako aj zlepšiť výmenu informácií, a to aj prostredníctvom vzdelávania, odbornej prípravy a cvičení. Osobitne ZDÔRAZŇUJE, že silné transatlantické partnerstvo v oblasti kybernetickej bezpečnosti prispieva k našej spoločnej bezpečnosti, stabilite a prosperite, a BERIE NA VEDOMIE ustanovenia o spolupráci v oblasti kybernetickej bezpečnosti v Dohode o obchode a spolupráci medzi EÚ a Spojeným kráľovstvom. PRIPOMÍNAJÚC kľúčové úspechy spolupráce medzi EÚ a NATO v oblasti kybernetickej bezpečnosti v rámci vykonávania spoločného vyhlásenia z Varšavy z roku 2016 a z Bruselu z roku 2018, opätovne zdôrazňuje význam rozšírenej, vzájomne sa posilňujúcej a prínosnej spolupráce prostredníctvom vzdelávania, odbornej prípravy, cvičení a koordinovanej reakcie na škodlivé kybernetické činnosti pri plnom rešpektovaní rozhodovacej autonómie a postupov oboch organizácií na základe zásad transparentnosti, reciprocity a inkluzívnosti.

28. S cieľom prispieť ku globálnemu, otvorenému, slobodnému, stabilnému a bezpečnému kybernetickému priestoru, ktorý má čoraz väčší význam pre pokračujúcu prosperitu, rast, bezpečnosť, blahobyt, prepojenosť a integritu našich spoločností, SA ZAVÄZUJE neustále sa zapájať do normotvorných procesov v medzinárodných organizáciách, najmä procesov súvisiacich s Prvým výborom OSN, poskytovať svoju podporu a prispievať k uznávaniu uplatňovania medzinárodného práva v kybernetickom priestore, ako aj dodržiavaniu noriem, pravidiel a zásad zodpovedného správania sa štátov v kybernetickom priestore, a to aj prostredníctvom rýchleho vytvorenia akčného programu pre zlepšenie zodpovedného správania sa štátov v kybernetickom priestore ako konštruktívneho, inkluzívneho a na konsenze založeného nadviazania na súčasné procesy skupiny vládnych expertov OSN (UN GGE) a otvorenej pracovnej skupiny OSN (OEWG).

29. PRIPOMÍNA svoje pevné odhodlanie presadzovať účinný multilateralizmus a globálny poriadok založený na pravidlách, ktorého jadrom je Organizácia Spojených národov, a svoje odhodlanie posilniť spoluprácu a koordináciu s medzinárodnými a regionálnymi organizáciami, konkrétne so systémom OSN, NATO, Radou Európy, OBSE, OECD, AÚ, OAŠ, ASEAN-om, Regionálnym fórom ASEAN-u, Radou pre spoluprácu v Perzskom zálive (GCC) a Ligou arabských štátov (LAŠ), pokiaľ ide o diskusie o kybernetických otázkach, ako aj pokračovanie a rozširovanie štruktúrovaných kybernetických dialógov a konzultácií EÚ s tretími krajinami. ZDÔRAZŇUJE svoju aktívnu podporu OSN, najmä v súvislosti s jej Agendou 2030 vrátane cieľov v oblasti udržateľného rozvoja, a VÍTA plán generálneho tajomníka OSN týkajúci sa digitálnej spolupráce a jeho program pre odzbrojenie, ktorými sa posilňuje zodpovednosť a dodržiavanie noriem v kybernetickom priestore a prispieva sa k predchádzaniu konfliktom vyplývajúcim zo škodlivej činnosti v kybernetickom priestore a k ich mierovému urovnávaniu. VÍTA návrh vysokého predstaviteľa pre zahraničné veci a bezpečnostnú politiku vytvoriť neformálnu sieť kybernetickej diplomacie EÚ s cieľom rozvíjať angažovanosť a odborné znalosti EÚ a členských štátov v medzinárodných kybernetických otázkach a zvýšiť tým koordinovaný vplyv.

30. So ZÁUJMOM OČAKÁVA nadchádzajúci návrh na preskúmanie politického rámca EÚ pre kybernetickú obranu (CDPF) a ZAVÄZUJE SA pokračovať v úsilí o posilnenie rozmerov kybernetickej bezpečnosti a kybernetickej obrany s cieľom zabezpečiť, aby boli plne integrované do širšej oblasti bezpečnosti a obrany, najmä v kontexte práce na Strategickom kompase. DOMNIEVA SA, že nadchádzajúca „Vojenská vízia a stratégia pre kybernetický priestor ako operačnú oblasť“ prispeje k prehĺbeniu týchto diskusií. VÍTA iniciatívu Európskej obrannej agentúry (EDA) na posilnenie spolupráce medzi vojenskými tímami CERT a PODPORUJE úsilie vynaložené na posilnenie civilno-vojenských synergických účinkov a koordinácie v oblasti kybernetickej obrany a kybernetickej bezpečnosti vrátane aspektov súvisiacich s kozmickým priestorom, a to aj prostredníctvom špecializovaných projektov PESCO.

31. VÍTA návrh vypracovať program EÚ na budovanie vonkajších kybernetických kapacít, návrh na vytvorenie rady EÚ pre budovanie kybernetických kapacít a zriadenie a zavedenie siete EU CyberNet (sieť EÚ na budovanie kybernetických kapacít) s cieľom zvýšiť kybernetickú odolnosť a kapacity na celom svete. V tejto súvislosti VÍTA spoluprácu s členskými štátmi, ako aj s partnermi z verejného a súkromného sektora, najmä s Globálnym fórom o kybernetických odborných znalostiach (GFCE) a inými príslušnými medzinárodnými orgánmi s cieľom zabezpečiť koordináciu a vyhnúť sa duplicite. Osobitne NABÁDA na spoluprácu s partnermi na západnom Balkáne a vo východnom a južnom susedstve EÚ.

32. S cieľom zabezpečiť, aby všetky krajiny mohli využívať sociálne, hospodárske a politické výhody internetu a využívania technológií, SA ZAVÄZUJE pomáhať partnerským krajinám pri riešení rastúceho problému škodlivých kybernetických činností, najmä tých, ktoré poškodzujú rozvoj ich hospodárstiev, spoločností a integritu a bezpečnosť demokratických systémov, a to aj v súlade s úsilím v rámci akčného plánu pre európsku demokraciu.

33. S cieľom zabezpečiť vypracovanie, vykonávanie a monitorovanie návrhov predložených v rámci stratégie kybernetickej bezpečnosti EÚ a s ohľadom na viacročný charakter niektorých iniciatív NABÁDA Komisiu a vysokého predstaviteľa pre zahraničné veci a bezpečnostnú politiku, aby vypracovali podrobný plán vykonávania, v ktorom sa stanovia priority a harmonogram plánovaných opatrení. Bude MONITOROVAŤ pokrok vo vykonávaní týchto záverov prostredníctvom akčného plánu, ktorý bude Rada pravidelne preskúmavať a aktualizovať v úzkej spolupráci s Európskou komisiou a vysokým predstaviteľom.