EURÓPSKA
KOMISIA

V Bruseli 29. 1. 2020
COM(2020) 50 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

Bezpečné zavádzanie 5G v EÚ – Vykonávanie súboru nástrojov

1. *Úvod*

Piata generácia telekomunikačných sietí (5G) má zohrávať dôležitú úlohu v rozvoji európskej spoločnosti a hospodárstva. Očakáva sa, že siete 5G ponúknu rozsiahle hospodárske príležitosti a budú dôležitým základom pre digitálnu a ekologickú transformáciu v oblastiach ako doprava, energetika, výroba, zdravotníctvo, poľnohospodárstvo a médiá.

Siete 5G preto potenciálne ovplyvnia takmer všetky aspekty života občanov Únie. Kybernetická bezpečnosť sietí 5G je preto nevyhnutná nielen na ochranu našich hospodárstiev, spoločností a demokratických procesov, ale aj na zabezpečenie dôveryhodnej digitálnej transformácie v prospech všetkých občanov Únie.

Závislosť mnohých kritických služieb od sietí 5G znamená, že dôsledky systémového a rozsiahleho narušenia by boli mimoriadne závažné a vzhľadom na vzájomné prepojenie digitálnych ekosystémov by mohli mať významný vplyv aj za hranicami jednotlivých štátov. V dôsledku toho je zabezpečenie kybernetickej bezpečnosti sietí 5G pre Úniu záležitosťou strategického významu, a to v čase, keď sú kybernetické útoky na vzostupe, keď sú sofistikovanejšie než kedykoľvek predtým a prichádzajú zo strany rozličných útočníkov, najmä z tretích krajín alebo zo štátom podporovaných útočníkov. Pokiaľ ide o bezpečnosť kritických infraštruktúr ako sú siete 5G, dospelo sa k rozhodnutiu po prvýkrát definovať spoločný európsky prístup. Tento prístup plne rešpektuje otvorenosť vnútorného trhu EÚ, pokiaľ sa dodržiavajú bezpečnostné požiadavky EÚ založené na riziku.

Európska rada 22. marca 2019 vyzvala na zosúladený prístup k bezpečnosti sietí 5G. Komisia 26. marca 2019 prijala odporúčanie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G[1]. V odporúčaní sa členské štáty vyzývajú, aby dokončili vnútroštátne posúdenie rizík, preskúmali vnútroštátne opatrenia a aby sa na úrovni EÚ spoločne podieľali na koordinovanom posúdení rizík a pripravili súbor nástrojov možných zmierňujúcich opatrení. Toto oznámenie je neoddeliteľnou súčasťou komplexnej európskej digitálnej stratégie Komisie tak, ako to požadovala Európska rada.

2. *Zavádzanie sietí 5G v EÚ*

Zavádzanie sieťovej infraštruktúry 5G v Európe je kľúčové pre európsku priemyselnú stratégiu a konkurencieschopnosť. Komisia uznala zavedenie sieťových technológií 5G za hlavný faktor umožňujúci budúce digitálne služby. Komisia prijala v roku 2016 akčný plán pre 5G s cieľom zabezpečiť, aby mala Únia od roku 2020 infraštruktúru konektivity potrebnú na svoju digitálnu transformáciu a na komplexné zavádzanie v mestských oblastiach a hlavných dopravných trasách do roku 2025[2]. V oznámení o gigabitovej spoločnosti sa stanovuje cieľ, aby existoval prístup k mobilnému dátovému pripojeniu kdekoľvek[3] vrátane vidieckych oblastí a vzdialených regiónov.

---

1 Odporúčanie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G, Ú. v. EÚ L 88, 29.3.2019, s. 42 – 47.

2 COM(2016) 588 zo 14. júna 2016 o 5G pre Európu: akčný plán.

3 COM(2016) 587 „Pripojenie pre konkurencieschopný jednotný digitálny trh – smerom k európskej gigabitovej spoločnosti“.

Pokiaľ ide o prideľovanie frekvencií, členské štáty pridelili 16 % priekopníckych pásiem 5G[4]. Vzhľadom na právnu povinnosť umožniť používanie všetkých priekopníckych pásiem 5G do konca roka sa konzultácie týkajúce sa viacerých postupov prideľovania očakávajú v najbližších niekoľkých mesiacoch.

Európa je jedným z najrozvinutejších regiónov na svete, pokiaľ ide o komerčné spustenie služieb 5G[5]. V súčasnosti sa očakáva, že prvé služby 5G budú k dispozícii v 138 európskych mestách do konca roka 2020. Prvé siete 5G sú založené na súčasnej štvrtej generácii (4G) sieťových technológií. Služby 5G sa poskytujú najmä širokej verejnosti, a to buď ako zlepšenie kapacity a rýchlosti 4G, alebo ako nákladovo efektívna bezdrôtová alternatíva k pevným sieťam[6].

Pokiaľ ide o príležitosti v oblasti nových služieb medzi podnikmi, napríklad v sektoroch energetiky, potravinárstva a poľnohospodárstva, zdravotnej starostlivosti, výroby alebo dopravy, Európa je značne popredu s investíciou vo výške 1 miliardy eur vrátane financovania EÚ vo výške 300 miliónov eur v kontexte verejno-súkromného partnerstva 5G v rámci programu Horizont 2020. Táto investícia pokrýva viac ako 160 rozsiahlych pokusných prevádzok siete 5G identifikovaných v Európe vrátane desiatich cezhraničných cestných koridorov na rozsiahle testovanie prepojených a automatizovaných služieb mobility založených na sieťach 5G. Pokusné prevádzky zahŕňajú aplikácie s podporou 5G v oblastiach od udržateľnej zdravotnej starostlivosti a automatizovanej mobility, poľnohospodárstva efektívne využívajúceho zdroje až po inteligentné elektrické siete a Priemysel 4.0. Okrem toho Európska investičná banka pomocou Európskeho fondu pre strategické investície poskytla úvery na urýchlenie výskumu a vývoja technológie 5G.

Európsky kódex elektronických komunikácií[7], ktorý sa bude uplatňovať od 21. decembra 2020, je dôležitým základom na vytvorenie priaznivého investičného prostredia nielen pre siete 5G. Okrem toho budú aj programy verejného financovania, ako je napríklad Nástroj na prepájanie Európy – Digitalizácia[8] alebo európske štrukturálne a investičné fondy, zohrávať dôležitú úlohu pri podpore budúceho zavádzania sietí 5G, a to najmä pripájaním komunít, ako sú školy, nemocnice, mestá a miestne správy, na služby s podporou 5G.

Vzhľadom na strategické možnosti Európy v oblasti služieb 5G pre rôzne odvetvia bude mimoriadne dôležité, aby prevádzkovatelia a poskytovatelia služieb investovali do moderných sietí 5G a riešení pre služby. Tie si budú vyžadovať nielen nové rádiové siete 5G, ale aj nové

---

4 http://www.5GObservatory.eu.

5 http://www.5GObservatory.eu.

6 Niektoré z nových funkcií 5G sa zavedú v súlade s fázovým prístupom. V prvej fáze (veľmi krátkej alebo krátkodobej) bude zavádzanie 5G pozostávať predovšetkým z „nie nezávislých“ sietí, v ktorých sa na technológiu 5G inovuje len rádiová prístupová sieť, a inak sa budú opierať o existujúce základné siete 4G. Koncovým používateľom sa tým umožní rozšírený výkon mobilného širokopásmového pripojenia. V nasledujúcich fázach (krátkodobé/strednodobé až dlhodobé) si zavádzanie „nezávislých“ sietí 5G vrátane funkcií základnej siete 5G bude vyžadovať oveľa rozsiahlejšiu zmenu sieťovej architektúry, a časom k nej bude viesť.

7 Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972, ktorou sa stanovuje európsky kódex elektronických komunikácií (prepracované znenie).

8 Návrh nariadenia COM(2018) 438 zo 6. júna 2018, ktorým sa zriaďuje Nástroj na prepájanie Európy a zrušujú sa nariadenia (EÚ) č. 1316/2013 a (EÚ) č. 283/2014.

takzvané nezávislé základné siete 5G, aby sa zabezpečili moderné funkcie 5G ako je network slicing[9] a edge computing[10].

Komisia bude naďalej plne podporovať úspešné zavedenie 5G v EÚ, a to aj prostredníctvom spolupráce s členskými štátmi a zainteresovanými stranami, s cieľom využiť príležitosti, ktoré ponúka 5G. Náležitá pozornosť sa bude venovať relevantným zdravotným aspektom založeným na zásade predbežnej opatrnosti[11] v spolupráci s príslušnými medzinárodnými organizáciami a vedeckou obcou.

3. Koordinované posúdenie rizík na úrovni EÚ v oblasti kybernetickej bezpečnosti sietí 5G

Každý členský štát dokončil v rámci spoločného úsilia skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti[12] vlastné vnútroštátne posúdenie rizík svojich sieťových infraštruktúr 5G a výsledky postúpil Komisii a agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) do začiatku júla 2019.

Na základe týchto vnútroštátnych posúdení rizík skupina pre spoluprácu v oblasti kybernetickej bezpečnosti tvorená zástupcami členských štátov, Komisie a agentúry ENISA uverejnila 9. októbra 2019 správu o koordinovanom posúdení rizík na úrovni EÚ v oblasti kybernetickej bezpečnosti sietí 5G[13]. V správe sa identifikujú hlavné hrozby a útočníci, najohrozenejšie aktíva a najzraniteľnejšie miesta (vrátane technických a iných druhov zraniteľných miest), ktoré majú vplyv na siete 5G. Na základe toho sa v správe uvádza aj niekoľko kategórií rizík strategického významu z hľadiska EÚ, ktoré sú znázornené konkrétnymi scenármi rizika odrážajúcimi príslušné kombinácie rôznych parametrov (zraniteľné miesta, hrozby a útočníci) vo vzťahu k rôznym aktívam (pozri dodatok).

Agentúra ENISA s cieľom doplniť túto správu a ďalej prispieť k súboru nástrojov vykonala špecializované mapovanie[14] panorámy hrozieb, ktoré pozostáva z podrobnej analýzy určitých technických aspektov, najmä z identifikácie aktív siete a hrozieb, ktoré ich ovplyvňujú.

V správe o koordinovanom posúdení rizík na úrovni EÚ sa zdôrazňuje niekoľko aspektov dôležitých pre siete 5G. Konkrétne:

a) Technologické zmeny, ktoré prinesú siete 5G, zvýšia mieru vystavenia útokom a počet možných miest vstupu pre útočníkov:

– rozšírené funkcie na okraji siete a menej centralizovaná architektúra než v predchádzajúcich generáciách mobilných sietí znamená, že niektoré funkcie základných sietí

9 5G network slicing umožňuje vysoký stupeň segmentácie rôznych vrstiev služieb na tej istej fyzickej sieti, čím sa zvyšujú možnosti poskytovania diferencovaných služieb v rámci celej siete.

10 Edge computing je paradigma distribuovaných výpočtových systémov, ktorá približuje výpočet a dátové úložisko potrebnému miestu a tým zlepšuje čas odozvy a šetrí šírku pásma.

11 Odporúčanie Rady 1999/519/ES z 12. júla 1999 o obmedzení vystavenia širokej verejnosti elektromagnetickým poliam (0 Hz až 300 GHz).

12 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (smernica NIS). Skupina pre spoluprácu v oblasti kybernetickej bezpečnosti bola zriadená smernicou NIS s cieľom zabezpečiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi EÚ v oblasti kybernetickej bezpečnosti.

13 https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

14 Správa agentúry ENISA o panoráme hrozieb pre siete 5G: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

môžu byť začlenené do iných častí sietí, čím sa zodpovedajúce zariadenie stane citlivejším (napr. základňové stanice alebo funkcie MANO),

– väčší softvérový podiel v zariadení 5G vedie k zvýšenému riziku spojenému s vývojom softvéru a s postupmi aktualizácie, vytvára nové riziká chýb v konfiguráciách a v bezpečnostnej analýze dáva dôležitejšiu rolu rozhodnutiam, ktoré spravil každý prevádzkovateľ mobilnej siete vo fáze zavádzania siete.

b) Vďaka týmto novým technologickým vlastnostiam sa budú môcť prevádzkovatelia mobilných sietí s väčšou istotou spoliehať na dodávateľov tretích strán a na ich úlohu v dodávateľskom reťazci 5G.

Tým sa na druhej strane zvýši počet možností útokov, ktoré by mohli zneužiť útočníci, najmä z tretích krajín alebo štátom podporovaní útočníci, a to vzhľadom na ich možnosti (úmysel a zdroje) útočiť proti telekomunikačným sieťam členských štátov EÚ, ako aj potenciálna závažnosť dôsledkov takýchto útokov.

V tomto kontexte zvýšenej miery vystavenia sa útokom zo strany dodávateľov tretích strán sa rizikový profil jednotlivých dodávateľov stane mimoriadne dôležitým, najmä ak má dodávateľ významnú prítomnosť v rámci sietí alebo oblastí.

c) Veľká závislosť od jediného dodávateľa zvyšuje vystavenie sa riziku jeho prípadného zlyhania a s tým spojené následky. Zhoršujú sa tým aj potenciálne následky nedostatkov alebo zraniteľných miest a možnosti, že ich využijú útočníci, najmä ak ide o závislosť od dodávateľa s vysokým stupňom rizika.

d) Ak niektoré z nových prípadov použitia plánovaných pre 5G prinesú výsledky, siete 5G budú predstavovať dôležitú súčasť dodávateľského reťazca mnohých dôležitých IT aplikácií a ako také budú mať nielen vplyv na požiadavky na dôvernosť a ochranu súkromia, ale aj integrita a dostupnosť týchto sietí sa z pohľadu EÚ stane hlavným problémom v oblasti národnej bezpečnosti a veľkou bezpečnostnou výzvou.

Zdroj: Koordinované posúdenie rizík na úrovni EÚ.

V správe o koordinovanom posúdení rizík na úrovni EÚ sa ďalej uvádza, že tieto výzvy vytvárajú nový bezpečnostný model, v dôsledku čoho je potrebné prehodnotiť súčasný politický a bezpečnostný rámec, ktorý sa vzťahuje na odvetvie 5G a jeho ekosystém, a nevyhnutné, aby členské štáty prijali potrebné zmierňujúce opatrenia.

Na účinné riešenie zistených rizík a posilnenie bezpečnosti a odolnosti sietí 5G je potrebný komplexný prístup, čo znamená zavedenie súboru kľúčových opatrení, ako aj súvisiacich podporných opatrení, ktoré môžu súčasne riešiť riziká. Koordinované posúdenie rizík na úrovni EÚ poskytlo základ na určenie zmierňujúcich opatrení, ktoré sa môžu uplatňovať na vnútroštátnej a európskej úrovni.

V záveroch Rady z 3. decembra 2019 sa podporili zistenia koordinovaného posúdenia rizík a zdôraznil sa „význam koordinovaného prístupu a účinného vykonávania tohto odporúčania s

cieľom zabrániť fragmentácii jednotného trhu“[15]. Rada na tento účel vyzvala členské štáty, Komisiu a agentúru ENISA, aby „prijali všetky potrebné opatrenia v rámci svojich právomocí na zaistenie bezpečnosti a integrity elektronických komunikačných sietí, najmä sietí 5G, aby naďalej konsolidovali koordinovaný prístup k riešeniu bezpečnostných výziev súvisiacich s technológiami 5G“.

4. Súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G

Skupina pre spoluprácu v oblasti kybernetickej bezpečnosti zverejnila 29. januára 2020 súbor nástrojov EÚ s opatreniami na zmiernenie rizika[16]. Zaoberá sa všetkými rizikami uvedenými v správe o koordinovanom posúdení rizík.

Súbor nástrojov EÚ identifikuje a opisuje súbor strategických a technických opatrení, ako aj príslušné podporné opatrenia na posilnenie ich účinnosti, ktoré sa môžu zaviesť s cieľom zmierniť zistené riziká. **Strategické opatrenia** sa vzťahujú na opatrenia týkajúce sa rozšírených regulačných právomocí orgánov, ktoré majú kontrolovať verejné obstarávanie a zavádzanie sietí, osobitné opatrenia na riešenie rizík súvisiacich s netechnickou zraniteľnosťou, ako aj možné iniciatívy na podporu udržateľného a rôznorodého dodávateľského a hodnotového reťazca 5G, aby sa zabránilo systémovým a dlhodobým rizikám vyplývajúcim zo závislosti. Medzi **technické opatrenia** patria opatrenia na posilnenie bezpečnosti sietí a zariadení 5G, a to riešením rizík vyplývajúcich z technológií, procesov, ľudských a fyzikálnych faktorov. Okrem toho sa v rámci každej rizikovej oblasti uvedenej v koordinovanom posúdení rizík na úrovni EÚ stanovujú **plány na zmiernenie rizika** na základe najúčinnejších opatrení.

Spomedzi nich sa v záveroch o súbore nástrojov EÚ, na ktorých sa dohodla skupina pre spoluprácu v oblasti kybernetickej bezpečnosti, odporúča súbor **kľúčových opatrení**, ktoré majú vykonávať všetky členské štáty a Komisia, a to takto:

Závery o súbore nástrojov EÚ

V súbore nástrojov EÚ sa stanovujú rozličné opatrenia a kroky, ktoré – ak sa náležite skombinujú a účinne vykonávajú – tvoria základ koordinovaného prístupu v tejto oblasti. Vzhľadom na širokú škálu rizikových oblastí identifikovaných v koordinovanom posúdení rizík na úrovni EÚ a ich rozličnú povahu naozaj nebude stačiť jediný druh opatrenia, ale na riešenie kľúčových rizikových oblastí bude skôr potrebný celý rad opatrení použitých vo vhodnej kombinácii.

Na základe posúdenia možných plánov na zmiernenie rizika a stanovenia najúčinnejších opatrení sa v tomto súbore nástrojov odporúča:

1. Všetky členské štáty by mali zabezpečiť, aby mali zavedené opatrenia (vrátane právomocí vnútroštátnych orgánov), ktoré by vhodne a úmerne reagovali na aktuálne zistené a budúce riziká, a najmä aby zaistili svoju schopnosť obmedziť, zakázať a/alebo uložiť osobitné požiadavky alebo podmienky podľa prístupu založeného na riziku na účely dodávok,

[15] Závery Rady č. 14517/19 z 3. decembra 2019 o význame 5G pre európske hospodárstvo a o potrebe znížiť riziká, ktoré súvisia s 5G, https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[16] Kybernetická bezpečnosť sietí 5G – súbor nástrojov EÚ s opatreniami na zmiernenie rizika, 29. január 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

zavádzania a prevádzky sieťových zariadení 5G na základe rozličných bezpečnostných dôvodov.

Mali by najmä:

 *posilniť **bezpečnostné požiadavky** pre prevádzkovateľov mobilných sietí (napr. prísne kontroly prístupu, pravidlá bezpečnej prevádzky a monitorovania, obmedzenia outsourcingu špecifických funkcií atď.),*

 *posúdiť rizikový profil dodávateľov. V dôsledku toho **uplatňovať príslušné obmedzenia pre dodávateľov, ktorí sa považujú za vysokorizikových – vrátane potrebných vylúčení v záujme účinného zmiernenia rizík – v prípade kľúčových aktív** vymedzených v koordinovanom posúdení rizík na úrovni EÚ ako kritické a citlivé (napr. funkcie základnej siete, funkcie sieťového riadenia a zosúladenia a funkcie prístupovej siete),*

 *zabezpečiť, aby mal každý prevádzkovateľ primeranú stratégiu viacerých dodávateľov s cieľom **zabrániť akejkoľvek veľkej závislosti** od jedného dodávateľa (alebo dodávateľov s podobným rizikovým profilom) **alebo ju obmedziť**, zabezpečiť primeranú rovnováhu dodávateľov na vnútroštátnej úrovni a **zabrániť závislosti od dodávateľov, ktorí sa považujú za vysokorizikových**. Patrí sem aj zabránenie akejkoľvek situácii odkázanosti na jediného dodávateľa, a to aj podporou väčšej interoperability zariadení.*

2. Európska komisia by spolu s členskými štátmi mala:

 *prispieť k zachovaniu **rôznorodého a udržateľného dodávateľského reťazca 5G** s cieľom zabrániť dlhodobej závislosti vrátane:*

*o plného využívania existujúcich nástrojov a prostriedkov EÚ, najmä preverovaním potenciálnych **priamych zahraničných investícií**, ktoré majú vplyv na kľúčové aktíva 5G, a zabraňovaním **narušeniam** trhu s dodávkami 5G vyplývajúcim z potenciálneho dumpingu alebo subvencií a*

*o ďalšieho posilnenia **kapacít EÚ v oblasti technológií 5G a technológií ďalších generácií**, a to využitím príslušných programov a financovania EÚ,*

 *prispieť k uľahčeniu koordinácie medzi členskými štátmi, pokiaľ ide o **normalizáciu**, aby sa dosiahli konkrétne bezpečnostné ciele a rozvíjali sa **príslušné systémy certifikácie na úrovni EÚ** s cieľom podporiť bezpečnejšie produkty a procesy.*

3. Aby sa zabezpečilo, že tento koordinovaný prístup obstojí v skúške času, mal by sa predĺžiť mandát skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti a malo by sa pokračovať v spolupráci s inými príslušnými orgánmi a subjektmi, najmä s cieľom:

 *pravidelne preskúmavať – s podporou Komisie a agentúry ENISA — **posúdenia rizík na vnútroštátnej úrovni a na úrovni EÚ** v oblasti bezpečnosti sietí 5G a sietí ďalších generácií, naďalej vypracúvať a zosúlaďovať použitú metodiku posudzovania a prispôsobovať sa vývoju technológie 5G,*

 *vykonávať podrobné a pravidelné **monitorovanie a hodnotenie vykonávania** súboru nástrojov na základe štruktúrovaného podávania správ členskými štátmi,*

 koordinovať a podporovať vykonávanie ***podporných opatrení****, ktoré si vyžadujú spoluprácu na úrovni EÚ, najmä pokiaľ ide o vypracovanie usmernení a výmenu najlepších postupov týkajúcich sa rôznych opatrení,*

 prípadne podporovať ďalšiu možnú koordináciu na úrovni EÚ, najmä na dosiahnutie ďalšieho zbližovania, ***pokiaľ ide o technické a organizačné bezpečnostné požiadavky pre prevádzkovateľov sietí****.*

Zdroj: súbor nástrojov EÚ.

V záveroch o súbore nástrojov sa preukazuje silné odhodlanie členských štátov spoločne reagovať na bezpečnostné výzvy sietí 5G. Má to zásadný význam pre bezpečnosť v rámci členských štátov a pre celú EÚ, pre národné hospodárstva, ako aj pre vnútorný trh EÚ a technologickú suverenitu Európy. Koordinované posúdenie rizík na úrovni EÚ a súbor nástrojov EÚ poukazujú na vysokú hodnotu kolektívnej práce, ktorá sa vykonala v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti, a na intenzívnu spoluprácu medzi zástupcami zo všetkých členských štátov, Komisiou a agentúrou ENISA.

Tento súbor nástrojov umožňuje spoločný prístup EÚ ku kybernetickej bezpečnosti sietí 5G, podporuje konzistentnosť na celom vnútornom trhu prostredníctvom politík a koordinácie EÚ, a umožňuje aj vykonávanie právomocí členských štátov, najmä pokiaľ ide o národnú bezpečnosť. Zmierňujúce opatrenia a zmierňujúce plány, ktoré obsahuje, umožňujú vhodnú, účinnú a primeranú reakciu EÚ na spoločné výzvy kybernetickej bezpečnosti sietí 5G.

Komisia víta zverejnenie súboru nástrojov EÚ pre kybernetickú bezpečnosť 5G a plne podporuje všetky uvedené závery.

Komisia vyzýva členské štáty a príslušné inštitúcie, agentúry a iné orgány Únie, aby:

i) zabezpečili rýchle vykonávanie účinných a vhodných stratégií na zmiernenie rizika v celej EÚ v súlade so súborom nástrojov EÚ a

ii) prijali všetky potrebné ďalšie kroky na zabezpečenie koordinácie na úrovni Únie, a to aj prostredníctvom ďalšieho úsilia v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti a vytvorením silného mechanizmu na monitorovanie vykonávania súboru nástrojov EÚ s cieľom zabezpečiť účinnosť opatrení a bezproblémové fungovanie vnútorného trhu.

5. Vykonávanie súboru nástrojov

Odhodlanie členských štátov plne využívať tento súbor nástrojov je nevyhnutné pre dôveryhodný a úspešný európsky prístup k bezpečnosti 5G. Zatiaľ čo členské štáty rozhodnú o vhodnosti konkrétneho opatrenia na základe vnútroštátnych okolností, je absolútne nevyhnutné, aby **bol v každom členskom štáte (a v prípade niektorých opatrení na úrovni EÚ) zavedený súbor kľúčových opatrení odporúčaných skupinou pre spoluprácu v oblasti kybernetickej bezpečnosti (pozri uvedené závery o súbore nástrojov)** s cieľom riešiť zistené riziká.

Komisia je pripravená aj naďalej poskytovať svoju plnú podporu počas nasledujúcich fáz a vyzýva členské štáty, aby:

– **do 30. apríla 2020** prijali konkrétne a merateľné kroky na vykonávanie súboru kľúčových opatrení odporúčaných v záveroch o súbore nástrojov EÚ,

– **do 30. júna 2020** vypracovali správu skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti o stave vykonávania týchto kľúčových opatrení v jednotlivých členských štátoch na základe pravidelného podávania správ a monitorovania, ktoré sa vykonávajú najmä v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti s podporou Komisie a agentúry ENISA.

5.1. Zosúladený prístup k dodávateľom 5G založený na riziku

Vzhľadom na konečný cieľ zaistiť bezpečnosť a odolnosť sietí 5G a ich udržateľnosť sa členské štáty dohodli, že je potrebné posúdiť rizikový profil jednotlivých dodávateľov a následne uplatňovať príslušné obmedzenia pre dodávateľov, ktorí sa považujú za vysokorizikových, vrátane potrebných vylúčení v záujme účinného zmiernenia rizík, pokiaľ ide o kľúčové aktíva, ako sa uvádza v súbore nástrojov. Komisia je pripravená podporiť členské štáty pri vykonávaní týchto opatrení.

S cieľom podporiť ich vykonávanie v celej EÚ poskytuje koordinované posúdenie rizík na úrovni EÚ a súbor nástrojov EÚ usmernenia týkajúce sa 1. posúdenia rizikového profilu dodávateľov[17] a 2. citlivosti sieťových prvkov a funkcií[18], ako aj iných aktív. Koordinované posúdenie rizík na úrovni EÚ a opatrenia týkajúce sa súboru nástrojov pokrývajú riziká súvisiace s dodávateľmi sieťových zariadení a sieťových služieb 5G. Nevzťahujú sa na iné produkty alebo služby, ktoré títo alebo iní dodávatelia môžu poskytovať.

Ako sa vymedzuje v odseku 2.37 koordinovaného posúdenia rizík na úrovni EÚ, rizikové profily jednotlivých dodávateľov možno posúdiť na základe niekoľkých faktorov.

Posúdenie rizikových profilov dodávateľov by sa malo vykonávať výlučne z bezpečnostných dôvodov a na základe objektívnych kritérií. S cieľom uľahčiť koordinovaný prístup k vykonávaniu týchto opatrení sa v súbore nástrojov odporúča, aby si členské štáty vymieňali informácie o vnútroštátnych prístupoch a najlepších postupoch. Komisia sa okrem toho domnieva, že toto opatrenie by malo byť jednou z hlavných priorít ďalšej fázy činnosti v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti, ako aj činnosti Komisie a agentúry ENISA.

Je dôležité, aby sa včas prijali obmedzenia týkajúce sa dodávateľov, ktorí sa považujú za vysokorizikových, vrátane potrebných vylúčení v záujme účinného zmiernenia rizík, ako aj opatrenia na zabránenie závislosti od týchto dodávateľov. Ak sa prijmú čo najskôr, a pokiaľ možno v súvislosti s postupmi udeľovania licencií na frekvencie 5G, zvýši sa aj predvídateľnosť pre účastníkov trhu, čím sa prispeje k rýchlemu zavádzaniu sietí 5G a zaistí sa dlhodobá bezpečnosť sietí 5G a odolnosť dodávateľského reťazca 5G.

Zároveň sa v rámci vnútroštátneho vykonávania týchto opatrení môžu, ak je to potrebné a odôvodnené, určiť rôzne časové rámce, najmä v prípade vysokého stupňa existujúcej

[17] Odsek 2.37 koordinovaného posúdenia rizík na úrovni EÚ.

[18] V odseku 2.21 koordinovaného posúdenia rizík na úrovni EÚ sa uvádzajú hlavné kategórie prvkov a funkcií a ich celková úroveň citlivosti a uvádza sa viacero kľúčových prvkov, ktoré členské štáty určili pre každú kategóriu. V odsekoch 2.28 a 2.29 sa uvádza niekoľko ďalších druhov citlivých aktív alebo oblastí (napr. konkrétne subjekty alebo zemepisné oblasti).

závislosti od zariadenia alebo služieb dodávateľov, ktorí sa posudzujú ako vysokorizikoví (napr. zohľadnením cyklov modernizácie zariadení, najmä migrácie sietí 5G od „nie nezávislých“ po „nezávislé“). Členské štáty by mohli zvážiť vymedzenie plánov vykonávania, ktoré by mohli zahŕňať primerané prechodné obdobia pre príslušných prevádzkovateľov sietí. V tejto súvislosti by sa prechodné obdobia mali vymedziť tak, aby sa zachovali, alebo dokonca posilnili stimuly na investovanie do moderných sieťových zariadení vrátane urýchlenia zavádzania plnofunkčných („nezávislých“) základných sietí 5G a nahradenia existujúcich zariadení 4G v iných častiach sietí (napr. v rádiovej prístupovej sieti) v súlade s cieľmi akčného plánu pre 5G[19].

Navyše vzhľadom na zložitosť sietí 5G založených na softvéri môžu telekomunikační prevádzkovatelia popri dodávkach sieťových zariadení čoraz viac využívať subjekty tretích strán na plnenie určitých úloh, ako je údržba a modernizácia sietí a softvéru 5G, ako aj ďalšie externe riadené služby. Ako sa uvádza v koordinovanom posúdení rizík na úrovni EÚ, toto predstavuje zdroj závažného bezpečnostného rizika. Preto by sa tomuto aspektu mala venovať osobitná pozornosť. Je nevyhnutné, aby sa vykonalo aj dôkladné posúdenie bezpečnosti rizikových profilov dodávateľov, ktorí sú týmito službami poverení, najmä ak sa tieto úlohy nevykonávajú v EÚ. Mali by sa prijať vhodné opatrenia vrátane uplatňovania obmedzení, najmä v citlivých častiach sietí 5G, alebo potrebného vylúčenia vysokorizikových subjektov v súlade so zmierňujúcimi opatreniami súboru nástrojov s cieľom zachovať dlhodobú integritu infraštruktúry 5G.

5.2. Úloha Komisie pri podpore vykonávania súboru nástrojov

Komisia bude naďalej podporovať vykonávanie prístupu EÚ ku kybernetickej bezpečnosti sietí 5G vo všeobecnosti, ako aj vykonávanie konkrétnych iniciatív v súvislosti s opatreniami a cieľmi súboru nástrojov, kde môže priniesť pridanú hodnotu. Komisia plne využije svoje právomoci a príslušné nástroje v rozsahu potrebnom na riešenie zistených bezpečnostných aspektov. Komisia sa tým, že koná spoločne s členskými štátmi a súkromným sektorom, usiluje podporovať strategické opatrenia, ktoré prispejú k zabezpečeniu technologickej suverenity a vedúceho postavenia EÚ v budúcom vývoji sieťových technológií, v oblasti technológií kybernetickej bezpečnosti a vo všetkých relevantných stavebných prvkoch, od ktorých závisí celé naše hospodárstvo a bezpečnosť.

S cieľom zabezpečiť vykonávanie príslušných zmierňujúcich opatrení v súbore nástrojov v oblastiach, ktoré patria do jej právomoci, Komisia vykoná konkrétne tieto kroky:

Zaručenie kybernetickej bezpečnosti sietí 5G a rôznorodého hodnotového reťazca 5G:

– **Spolupráca v oblasti kybernetickej bezpečnosti**: Pokračovať v poskytovaní podpory členským štátom na účinné, koordinované a včasné vykonávanie vnútroštátnych opatrení prostredníctvom skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti.

– **Pravidlá týkajúce sa telekomunikácií a kybernetickej bezpečnosti**: Poskytovať podporu vykonávania opatrení súboru nástrojov súvisiacich s bezpečnostnými požiadavkami, najmä pokiaľ ide o príslušné ustanovenia európskych pravidiel v oblasti elektronických komunikácií, a zohľadňovať pridanú hodnotu možných vykonávacích aktov, v ktorých sa podrobne uvádzajú technické a organizačné bezpečnostné opatrenia, s cieľom doplniť vnútroštátne

[19] COM(2016) 588 zo 14. septembra 2016 o 5G pre Európu: akčný plán.

predpisy a zvýšiť účinnosť a konzistentnosť bezpečnostných opatrení uložených prevádzkovateľom.

– **Normalizácia**: Prijať opatrenia s cieľom pomôcť udržať a prípadne zvýšiť európsku účasť v príslušných normalizačných orgánoch, aby sa dosiahli ciele Európy v oblasti bezpečnosti a interoperability. Komisia spolu s členskými štátmi najmä posúdi a podporí technické špecifikácie a normy, ktoré umožnia interoperabilitu medzi dodávateľmi zariadení 5G v rôznych častiach siete, a to aj v tradičných sieťach, s cieľom umožniť skutočné prostredie s viacerými dodávateľmi, napríklad prostredníctvom otvorených interoperabilných rozhraní.

– **Certifikácia**: Podporovať rozvoj systémov certifikácie 5G, ktoré riešia potreby sietí 5G v európskom rámci pre certifikáciu kybernetickej bezpečnosti.

– **Preverovanie priamych zahraničných investícií**: Podporovať vykonávanie rámca EÚ na preverovanie, a to mapovaním hodnotového reťazca 5G vrátane citlivých sieťových aktív a pravidelným monitorovaním priamych zahraničných investícií v celom hodnotovom reťazci. Komisia bude v súlade s harmonogramom preverovania priamych zahraničných investícií (od októbra 2020) kontrolovať zahraničné investície v oblasti 5G v súlade s usmerneniami stanovenými v nariadení (EÚ) 2019/452, pričom zohľadní koordinované posúdenie rizík na úrovni EÚ a súbor nástrojov EÚ.

– **Nástroje na ochranu obchodu**: Monitorovať všetok relevantný vývoj na trhu v EÚ a v tretích krajinách a opatreniami na ochranu obchodu chrániť účastníkov z EÚ na európskom trhu 5G s cieľom riešiť potenciálne praktiky narúšajúce obchod (dumping alebo subvencovanie), v prípade potreby aj začatím predbežných vyšetrovaní.

– Pravidlá hospodárskej súťaže: Monitorovať fungovanie trhov s dodávkami hardvéru a softvéru 5G s cieľom zabezpečiť, aby priniesli výsledky v oblasti hospodárskej súťaže, a to aj v súvislosti s možnou zmluvnou alebo technickou situáciou odkázanosti na určitého dodávateľa.

– **Programy financovania EÚ**: Zabezpečiť, aby účasť na programoch financovania EÚ v príslušných technologických oblastiach bola podmienená splnením bezpečnostných požiadaviek, a to plným využívaním a ďalším vykonávaním bezpečnostných podmienok v programoch výskumu a inovácie, najmä v programe Horizont Európa, programe Digitálna Európa a v rámci Nástroja na prepájanie Európy 2, v európskych štrukturálnych a investičných fondoch a v iných príslušných programoch. Podobný prístup by sa mal zaujať aj v rámci programov vonkajšieho financovania a finančných nástrojov EÚ, a to aj pokiaľ ide o financovanie poskytované prostredníctvom medzinárodných finančných inštitúcií.

– Verejné obstarávanie: Využívať verejné obstarávania v oblasti sietí 5G s cieľom podporiť identifikované ciele v oblasti bezpečnosti, rozmanitosť dodávateľov a dlhodobú udržateľnosť sietí 5G. Usilovať sa najmä o náležité zohľadňovanie bezpečnostných aspektov pri zadávaní verejných zákaziek týkajúcich sa sietí 5G v súlade s pravidlami EÚ v oblasti verejného obstarávania.

– **Reakcia na incidenty a krízové riadenie (koncepcia) a kybernetické cvičenia**: Naplno využiť zavedenie koncepcie[20] koordinovanej reakcie EÚ na kybernetické incidenty veľkého

[20] Odporúčanie Komisie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu.

rozsahu. Okrem toho spolu s agentúrou ENISA zvážiť možnosť uskutočnenia kybernetického cvičenia 5G, akonáhle to umožní vyspelosť trhu.

A pod vedením vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku a podpredsedu Komisie a pod vedením Rady:

– **Rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti (súbor nástrojov kybernetickej diplomacie)**[21]: V prípade škodlivých kybernetických činností, ktoré ohrozujú integritu a bezpečnosť EÚ, sa členské štáty vyzývajú, aby využívali príslušné opatrenia spoločnej zahraničnej a bezpečnostnej politiky v rámci súboru nástrojov kybernetickej diplomacie EÚ (prípadne vrátane reštriktívnych opatrení) s cieľom podporiť spoluprácu, uľahčiť zmierňovanie hrozieb a ovplyvniť správanie potenciálnych útočníkov.

Okrem toho viacero programov prispeje k cieľom zabrániť riziku dlhodobej závislosti alebo ho obmedziť tým, že podporí rôznorodý a udržateľný trh pre 5G, a to aj zachovaním kapacít EÚ v hodnotovom reťazci 5G a investovaním do inovácie v súlade s medzinárodnými záväzkami EÚ.

Podpora inovácie a investícií do kybernetickej bezpečnosti a do technológií sieťovej infraštruktúry:

– **Programy** financovania EÚ: Zvýšiť investície do výskumu, inovácie a zavádzania sieťových technológií a príslušných základných stavebných prvkov. Komisia navrhla v rámci budúceho rozpočtu EÚ na obdobie 2021 – 2027 investície do technológií kybernetickej bezpečnosti vo výške takmer 3 miliardy eur. Patrí sem výskum a inovácia v rámci programu Horizont Európa a podpora spôsobilostí v oblasti kybernetickej bezpečnosti v rámci programu Digitálna Európa. Program InvestEU môže takisto poskytovať finančnú podporu na výskum a vývoj v oblasti 5G, ako aj podporu pri zavádzaní 5G.

Okrem toho Komisia v rámci budúceho programu Horizont Európa[22] navrhla zriadenie inštitucionalizovaného partnerstva EÚ v oblasti internetu novej generácie/6G (inteligentné siete a služby) v spolupráci s priemyslom a koordináciou s členskými štátmi s cieľom dokončiť zavádzanie sietí 5G, a najmä **pripraviť sa na 6G** – budúcu generáciu mobilných technológií. Z rozpočtu EÚ (2021 – 2027) boli navrhnuté investície EÚ vo výške viac ako 2,5 miliardy eur, pričom túto iniciatívu má doplniť aspoň 7,5 miliardy eur súkromných investícií.

– **Priemyselný rozvoj a využitie**: Vyhodnotiť možné nedostatky alebo zlyhania trhu v rámci hodnotového reťazca 5G, ktoré by v súlade s návrhmi fóra dôležitých projektov spoločného európskeho záujmu na vysokej úrovni odôvodňovali cielené intervencie v rámci nasledujúceho dlhodobého rozpočtu alebo možné dôležité projekty spoločného európskeho záujmu v oblasti kybernetickej bezpečnosti. Rozhodnutie navrhnúť a zriadiť dôležité projekty spoločného európskeho záujmu je v rukách členských štátov a spoločností. Pravidlá EÚ poskytujú podporný rámec a Komisia je pripravená uľahčovať potrebné kontakty a poskytovať usmernenia.

[21] Závery Rady č. 9916/17 z 20. novembra 2017.

[22] Financovanie sa môže poskytnúť aj prostredníctvom programu Nástroj na prepájanie Európy 2.0 a programu Digitálna Európa.

6. Záver

Siete 5G majú priniesť celý rad príležitostí pre európskych občanov, spoločnosť a hospodárstvo. Zaistenie bezpečnosti a odolnosti sietí 5G je preto nevyhnutné. Kybernetické hrozby (vrátane rizika interferencie zo strany útočníkov z tretích krajín alebo štátom podporovaných útočníkov) sú však neustále sa vyvíjajúcou výzvou, ktorej závažnosť sa zvyšuje s rastúcou závislosťou od technológií a údajov. Zanedbaním kybernetickej bezpečnosti by sa oslabila dôvera v rozvoj digitálneho hospodárstva a spoločnosti a Únia by nemohla naplno využívať jeho výhody. Treba, aby sa reakcia zodpovedajúcim spôsobom vyvíjala a posilňovala.

Koordinovaný a konzistentný prístup ku kybernetickej bezpečnosti v EÚ pre kritické technológie a siete má pre EÚ zásadný význam, aby si zabezpečila technologickú suverenitu a aby si udržala a rozvíjala priemyselné kapacity. Komisia plne podporí vykonávanie prístupu EÚ ku kybernetickej bezpečnosti sietí 5G a zároveň zabezpečí, aby trhy EÚ zostali otvorené pre produkty a služby, ktoré sú v súlade s vyvíjajúcimi sa požiadavkami na kybernetickú bezpečnosť a dôveru.

Na tento účel je dôležité, aby sa všetky zainteresované strany naďalej výrazne angažovali v oblasti bezpečnosti sietí 5G, čo si bude vyžadovať ďalšiu spoluprácu medzi členskými štátmi, Komisiou a agentúrou ENISA.

Ako sa uvádza vyššie, ďalším bezprostredným krokom Komisie bude vyzvať členské štáty, aby urýchlene podnikli kroky na účinné a objektívne vykonávanie opatrení, ktoré sa dohodli ako súčasť súboru nástrojov, a aby s podporou Komisie a agentúry ENISA naďalej spolupracovali s cieľom zabezpečiť koordináciu na úrovni EÚ. Komisia zároveň zavedie všetky príslušné opatrenia v rámci svojej právomoci, aby podporila vykonávanie súboru nástrojov zo strany členských štátov a posilnila jeho vplyv.

Dodatok: Rizikové kategórie (zdroj: koordinované posúdenie rizík na úrovni EÚ).

	Kategórie rizika
Scenáre rizika týkajúce sa nedostatočných bezpečnostných opatrení	*R1: Nesprávna konfigurácia sietí*
	R2: Chýbajúce kontroly prístupu
Scenáre rizika týkajúce sa dodávateľského reťazca 5G	*R3: Nízka kvalita produktu*
	R4: Závislosť od akéhokoľvek jediného dodávateľa v rámci jednotlivých sietí alebo nedostatočná rozmanitosť na celoštátnej úrovni
Scenáre rizika týkajúce sa spôsobu práce hlavných útočníkov	*R5: Zasahovanie štátu cez dodávateľský reťazec 5G*
	R6: Využívanie sietí 5G na organizovanú trestnú činnosť alebo zločineckou skupinou zameranou na koncových používateľov
Scenáre rizika týkajúce sa vzájomnej závislosti medzi sieťami 5G a inými kritickými systémami	*R7: Závažné narušenie kritickej infraštruktúry alebo služieb*
	R8: Hromadné zlyhanie sietí v dôsledku prerušenia dodávok elektrickej energie alebo iných podporných systémov
Scenáre rizika týkajúce sa zariadení koncového používateľa	*R9: Využívanie internetu vecí*