KOMISJA
EUROPEJSKA

Bruksela, dnia 29.1.2020 r.
COM(2020) 50 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi

1. *Wprowadzenie*

Sieci telekomunikacyjne piątej generacji (5G) będą odgrywać zasadniczą rolę w rozwoju europejskiego społeczeństwa i europejskiej gospodarki. Oczekuje się, że zapewnią one ogromne możliwości gospodarcze i stanowić będą istotny fundament transformacji cyfrowej i ekologicznej w obszarach takich jak transport, energetyka, produkcja, zdrowie, rolnictwo i media.

Technologia 5G będzie zatem miała potencjalny wpływ na niemal wszystkie aspekty życia obywateli UE. Cyberbezpieczeństwo sieci 5G ma więc decydujące znaczenie nie tylko dla ochrony naszych gospodarek, społeczeństw i procesów demokratycznych, ale także dla zapewnienia godnej zaufania transformacji cyfrowej z korzyścią dla wszystkich obywateli Unii.

Jeżeli wiele usług o krytycznym znaczeniu będzie uzależnionych od sieci 5G, zakłócenia o charakterze systemowym na wielką skalę będą miały szczególnie dotkliwe skutki, a ze względu na wzajemne połączenia ekosystemów cyfrowych mogłyby one mieć poważne konsekwencje wykraczające poza granice poszczególnych państw. W rezultacie zapewnienie cyberbezpieczeństwa sieci 5G jest kwestią o znaczeniu strategicznym dla Unii, w czasie gdy cyberataki nasilają się, są bardziej wyrafinowane niż kiedykolwiek wcześniej i stoi za nimi wielu różnych agresorów, w szczególności podmiotów pochodzących z państw spoza UE lub wspieranych przez państwa obce. Jeżeli chodzi o bezpieczeństwo infrastruktury krytycznej takiej jak 5G, wybrane rozwiązanie zakłada opracowanie – po raz pierwszy – wspólnego europejskiego podejścia. Podejście to w pełni gwarantuje zachowanie otwartego charakteru rynku wewnętrznego UE pod warunkiem przestrzegania unijnych wymogów bezpieczeństwa opartych na analizie ryzyka.

W dniu 22 marca 2019 r. Rada Europejska wezwała do przyjęcia wspólnego podejścia do bezpieczeństwa sieci 5G. Następnie w dniu 26 marca 2019 r. Komisja przyjęła zalecenie (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G[1]. W zaleceniu wezwano państwa członkowskie do ukończenia krajowych ocen ryzyka i przeprowadzenia przeglądu środków krajowych, do współpracy na szczeblu UE w zakresie skoordynowanej oceny ryzyka oraz do przygotowania wspólnego zestawu narzędzi obejmującego środki ograniczające ryzyko. Niniejszy komunikat stanowi integralną część kompleksowej europejskiej strategii cyfrowej opracowanej przez Komisję w odpowiedzi na apel Rady Europejskiej.

2. *Wprowadzenie sieci 5G w UE*

Wdrożenie w Europie infrastruktury na potrzeby sieci 5G ma zasadnicze znaczenie dla europejskiej strategii przemysłowej i konkurencyjności europejskich przedsiębiorstw. Komisja uznała wdrożenie technologii sieciowych 5G za główny czynnik umożliwiający świadczenie przyszłych usług cyfrowych. W 2016 r. Komisja przyjęła plan działania w zakresie sieci 5G, który ma zagwarantować, że od 2020 r. Unia posiadać będzie infrastrukturę łączności niezbędną do dokonania transformacji cyfrowej oraz do kompleksowego wdrożenia tej nowej technologii na obszarach miejskich i wzdłuż głównych tras transportowych do 2025 r.[2] W komunikacie w sprawie społeczeństwa gigabitowego

[1] Zalecenie (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G, Dz.U. L 88 z 29.3.2019, s. 42.
[2] COM(2016) 588 z dnia 14 września 2016 r., „Sieć 5G dla Europy: plan działania”.

sformułowano ambitny cel, zgodnie z którym dostęp do internetu ruchomego należy zapewnić wszędzie[3], w tym na obszarach wiejskich i oddalonych.

Jeżeli chodzi o przydział częstotliwości, państwa członkowskie przydzieliły 16 % pionierskich pasm sieci 5G[4]. Oczekuje się, że w ciągu najbliższych kilku miesięcy przeprowadzone zostaną konsultacje w sprawie szeregu procedur przydziału częstotliwości, gdyż państwa członkowskie są prawnie zobowiązane, by do końca roku umożliwić korzystanie z wszystkich pionierskich pasm sieci 5G.

Europa jest jednym z najbardziej zaawansowanych na świecie regionów, jeśli chodzi o komercyjne uruchomienie usług 5G[5]. Obecnie oczekuje się, że pierwsze usługi 5G będą dostępne w 138 europejskich miastach do końca 2020 r. Pionierskie sieci 5G opierają się na obecnej 4. generacji (4G) technologii sieciowych, a usługi 5G świadczone są głównie dla ogółu społeczeństwa – albo jako usprawnienie w stosunku do sieci 4G pod względem przepustowości i prędkości, albo jako korzystna cenowo bezprzewodowa alternatywa dla sieci stacjonarnych[6].

Jeżeli chodzi o nowe możliwości w kontekście nowych usług świadczonych między przedsiębiorstwami, takich jak usługi w sektorach energii, żywności i rolnictwa, opieki zdrowotnej, produkcji czy transportu, Europa jest na zaawansowanym etapie, realizując inwestycje rzędu 1 mld EUR, w tym 300 mln EUR z funduszy UE w kontekście partnerstwa publiczno-prywatnego w dziedzinie 5G w ramach programu „Horyzont 2020". Inwestycje te obejmują ponad 160 zakrojonych na szeroką skalę programów pilotażowych 5G zidentyfikowanych w Europie, w tym dziesięć transgranicznych korytarzy drogowych do celów prowadzonych na dużą skalę testów usług w technologii 5G z zakresu opartej na sieci i zautomatyzowanej mobilności. Testy te obejmują zastosowania 5G w obszarach takich jak zrównoważona opieka zdrowotna i zautomatyzowane rozwiązania z zakresu mobilności na potrzeby rolnictwa efektywnie korzystającego z zasobów czy też inteligentne sieci energii elektrycznej i przemysł 4.0. Ponadto EBI, wspierany przez Europejski Fundusz na rzecz Inwestycji Strategicznych, udzielił pożyczek na przyspieszenie działań badawczo-rozwojowych w zakresie technologii 5G.

Europejski kodeks łączności elektronicznej (zwany dalej „kodeksem")[7], który zacznie obowiązywać od dnia 21 grudnia 2020 r., stanowi ważną podstawę do stworzenia warunków sprzyjających inwestycjom w sieci 5G i nie tylko. Ponadto programy finansowania publicznego, takie jak instrument „Łącząc Europę – technologie cyfrowe"[8] lub europejskie

[3] COM(2016) 587 „Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego".

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

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

[6] Niektóre z nowych funkcjonalności sieci 5G zostaną wprowadzone etapowo. W pierwszej fazie (bardzo krótkiej lub krótkoterminowej) wprowadzanie sieci 5G będzie przebiegać przede wszystkim w oparciu o „niesamodzielne" sieci: do standardu 5G zostanie zmodernizowana tylko sieć dostępu radiowego, a pozostałe aspekty funkcjonowania sieci nadal będą opierać na istniejących sieciach szkieletowych 4G, które zapewnią użytkownikom końcowym większe prędkości dostępu do internetu za pośrednictwem mobilnych usług szerokopasmowych. W kolejnych fazach (krótko-/średnioterminowe do długoterminowych) wdrożenie „samodzielnych" sieci 5G, w tym funkcji sieci szkieletowej 5G, będzie wymagało – i z czasem przyczyni się do – znacznie większych zmian w architekturze sieci.

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona).

[8] Wniosek COM(2018) 438 z dnia 6 czerwca 2018 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego instrument „Łącząc Europę" oraz uchylającego rozporządzenia (UE) nr 1316/2013 i (UE) nr 283/2014.

fundusze strukturalne i inwestycyjne będą również miały zasadnicze znaczenie dla wsparcia przyszłego wdrożenia sieci 5G, w szczególności poprzez przyłączanie obiektów takich jak szkoły, szpitale, miasta i urzędy lokalne do sieci 5G i udostępnianie im usług oferowanych w oparciu o te sieci.

Biorąc pod uwagę strategiczne szanse, jakie usługi 5G niosą dla różnych gałęzi przemysłu w Europie, niezwykle istotne jest zadbanie o to, by operatorzy i dostawcy usług inwestowali w zaawansowane rozwiązania sieciowe i usługi 5G. Będą one wymagać nie tylko nowych sieci radiowych 5G, ale również nowych tzw. „samodzielnych" sieci szkieletowych 5G, aby zapewnić zaawansowane funkcje 5G, takie jak warstwowanie sieci[9] czy przetwarzanie danych na obrzeżach sieci (ang. *edge computing*)[10].

Komisja będzie nadal w pełni wspierać udane wprowadzanie sieci 5G w UE, w tym poprzez współpracę z państwami członkowskimi i zainteresowanymi stronami w celu wykorzystania możliwości oferowanych przez 5G. W oparciu o zasadę ostrożności[11] należycie uwzględnione zostaną odpowiednie aspekty zdrowotne, we współpracy z odpowiednimi organizacjami międzynarodowymi i środowiskiem naukowym.

3. Unijna skoordynowana ocena ryzyka dotycząca cyberbezpieczeństwa w sieciach 5G

Działając wspólnie w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji[12], każde państwo członkowskie ukończyło swoją krajową ocenę ryzyka dotyczącą infrastruktury sieci 5G i przekazało jej wyniki Komisji i ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) do lipca 2019 r.

Na podstawie tych krajowych ocen ryzyka w dniu 9 października 2019 r. grupa współpracy ds. bezpieczeństwa sieci i informacji, złożona z przedstawicieli państw członkowskich, Komisji i ENISA, opublikowała sprawozdanie na temat unijnej skoordynowanej oceny ryzyka w zakresie cyberbezpieczeństwa w sieciach 5G[13]. W sprawozdaniu tym wskazano główne rodzaje i źródła zagrożeń, najbardziej wrażliwe aktywa, główne luki (w tym zagrożenia techniczne i luki innego rodzaju) mające wpływ na sieci 5G. Na tej podstawie w sprawozdaniu wskazano również szereg kategorii ryzyka o znaczeniu strategicznym z perspektywy UE, zilustrowanych konkretnymi scenariuszami ryzyka, które odzwierciedlają odpowiednie kombinacje różnych parametrów (luk, zagrożeń i agresorów) w odniesieniu do różnych aktywów (zob. załącznik).

[9] Warstwowanie sieci 5G umożliwia zapewnienie wysokiego stopnia separacji między różnymi warstwami usług w tej samej sieci fizycznej, zwiększając tym samym możliwości oferowania zróżnicowanych usług w całej sieci.

[10] *Edge computing* jest modelem rozproszonego przetwarzania danych, w którym przetwarzanie i przechowywanie danych ma miejsce możliwie najbliżej lokalizacji, w której usługi te są potrzebne, co skraca czas odpowiedzi serwera i pozwala zaoszczędzić pasmo.

[11] Zalecenie Rady z dnia 12 lipca 1999 r. w sprawie ograniczenia narażenia ludności na pola elektromagnetyczne (od 0 Hz do 300 GHz) (1999/519/WE).

[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji). Grupa współpracy ds. bezpieczeństwa sieci i informacji została ustanowiona na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji w celu zapewnienia strategicznej współpracy i wymiany informacji między państwami członkowskimi UE w dziedzinie cyberbezpieczeństwa.

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

Jako uzupełnienie tego sprawozdania i dalszy wkład w zestaw narzędzi ENISA przygotowała specjalne opracowanie dotyczące krajobrazu zagrożeń[14], obejmujące szczegółową analizę niektórych aspektów technicznych, w szczególności identyfikację aktywów sieciowych i dotyczących ich zagrożeń.

W sprawozdaniu z unijnej skoordynowanej oceny ryzyka zwrócono uwagę na szereg aspektów mających znaczenie dla sieci 5G. W szczególności:

a) zmiany technologiczne wprowadzone przez 5G zwiększą ogólną powierzchnię ataku oraz liczbę punktów, w których sieć może zostać zaatakowana:

- większa funkcjonalność na obrzeżach sieci i mniej scentralizowana architektura niż w sieciach telefonii ruchomej poprzednich generacji oznaczają, że niektóre funkcje sieci szkieletowych mogą być elementem innych części sieci, co sprawia, że odnośny sprzęt staje się bardziej wrażliwy (np. stacje bazowe lub funkcje MANO);

- większe znaczenie oprogramowania w urządzeniach 5G podnosi ryzyko związane z procesem tworzenia i aktualizacji oprogramowania, stwarza nowe zagrożenia związane z konfiguracją oprogramowania i sprawia, że w kontekście analizy bezpieczeństwa zwiększa się rola wyborów dokonywanych przez każdego operatora sieci łączności ruchomej w fazie wdrażania sieci;

b) te nowe funkcje technologiczne będą miały większe znaczenie w kontekście uzależnienia operatorów sieci ruchomej od dostawców zewnętrznych i ich roli w łańcuchu dostaw 5G.

To z kolei zwiększy liczbę ścieżek ataku, które mogą być wykorzystane przez agresorów, w szczególności przez podmioty z państw spoza UE lub wspierane przez państwa obce, z uwagi na ich zdolności (zamiar i zasoby) przeprowadzania ataków na sieci telekomunikacyjne państw członkowskich UE, a także ze względu na potencjalną dotkliwość skutków takich ataków.

W tym kontekście zwiększonego narażenia na ataki, ułatwiane przez dostawców zewnętrznych, szczególnego znaczenia nabierze indywidualny profil ryzyka dostawcy, w szczególności wówczas, gdy sprzęt dostawcy jest obecny na znaczną skalę w danych sieciach lub na danych obszarach;

c) znaczna zależność od jednego dostawcy zwiększa ryzyko, jakie niesie potencjalne niewywiązanie się przez dostawcę z jego zobowiązań, oraz związane z tym skutki. Zaostrza również potencjalne skutki wynikające z istniejących słabości i luk, a także ewentualnego wykorzystania tych słabości i luk przez agresorów, w szczególności gdy dysponenci infrastruktury uzależnieni są od dostawcy stwarzającego wysokie ryzyko;

d) jeżeli niektóre z nowych zastosowań przewidzianych dla sieci 5G urzeczywistnią się, sieci 5G staną się ważną część łańcucha dostaw wielu kluczowych zastosowań informatycznych i w ten sposób nie tylko oddziaływać będą na wymogi dotyczące poufności i prywatności, ale również sprawią, że integralność i dostępność tych sieci stanie się istotną kwestią

[14] Sprawozdanie ENISA dotyczące krajobrazu zagrożeń w sieciach 5G: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

bezpieczeństwa narodowego i poważnym wyzwaniem w zakresie bezpieczeństwa z punktu widzenia UE.

Źródło: Unijna skoordynowana ocena ryzyka

W sprawozdaniu z unijnej skoordynowanej oceny ryzyka stwierdzono ponadto, że wyzwania te tworzą nowy paradygmat bezpieczeństwa, co sprawia, że konieczne jest dokonanie ponownej oceny obecnych ram polityki i bezpieczeństwa mających zastosowanie do sektora 5G i jego ekosystemu, a także powoduje konieczność zastosowania przez państwa członkowskie niezbędnych środków ograniczających ryzyko.

W celu skutecznego przeciwdziałania zidentyfikowanym zagrożeniom oraz wzmocnienia bezpieczeństwa i odporności sieci 5G konieczne jest kompleksowe podejście, co wiąże się z wprowadzeniem zestawu kluczowych środków, a także powiązanych działań wspierających, które mogą jednocześnie przeciwdziałać wspomnianym zagrożeniom. Unijna skoordynowana ocena ryzyka stanowi podstawę do określenia środków ograniczających ryzyko, które mogą być stosowane na szczeblu krajowym i europejskim.

W konkluzjach Rady z dnia 3 grudnia 2019 r. poparto ustalenia zawarte w skoordynowanej ocenie ryzyka i podkreślono „jak ważne jest skoordynowane podejście i skuteczne wdrażanie zalecenia, aby uniknąć fragmentacji jednolitego rynku”[15]. W tym celu Rada wezwała państwa członkowskie, Komisję i ENISA, by „w ramach swoich kompetencji podjęły wszelkie niezbędne działania w celu zapewnienia bezpieczeństwa i integralności sieci łączności elektronicznej, w szczególności sieci 5G, oraz w dalszym ciągu utrwalały skoordynowane podejście do wyzwań w zakresie bezpieczeństwa związanych z technologiami 5G”.

4. Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G

W dniu 29 stycznia 2020 r. grupa współpracy ds. bezpieczeństwa sieci i informacji opublikowała zestaw unijnych narzędzi służących ograniczeniu ryzyka[16]. Wspomniany zestaw narzędzi stanowi odpowiedź na wszystkie rodzaje ryzyka wskazane w sprawozdaniu ze skoordynowanej oceny ryzyka.

W unijnym zestawie narzędzi wskazano i opisano zestaw środków strategicznych i technicznych, jak również odpowiednie działania wspierające w celu zwiększenia ich skuteczności, które mogą zostać wprowadzone w celu ograniczenia zidentyfikowanych rodzajów ryzyka. **Środki strategiczne** obejmują środki dotyczące przyznanych organom zwiększonych uprawnień regulacyjnych do kontroli zamówień publicznych na urządzenia sieciowe oraz procesu wdrażania sieci, szczególne środki służące wyeliminowaniu zagrożeń związanych ze słabymi punktami o charakterze nietechnicznym, jak również możliwe inicjatywy mające na celu promowanie zrównoważonego i zróżnicowanego łańcucha dostaw i wartości 5G w celu uniknięcia ryzyka systemowego i ryzyka długoterminowego uzależnienia od konkretnych dostawców. **Środki techniczne** obejmują środki mające na celu zwiększenie bezpieczeństwa sieci i urządzeń 5G poprzez przeciwdziałanie ryzyku, którego źródłem są technologie, procesy, czynniki ludzkie i fizyczne. Ponadto w odniesieniu do

[15] Konkluzje Rady w sprawie znaczenia 5G dla gospodarki europejskiej oraz potrzeby ograniczenia zagrożeń dla bezpieczeństwa związanych z 5G. 3 grudnia 2019 r., 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[16] Cyberbezpieczeństwo sieci 5G – unijny zestaw narzędzi służących ograniczeniu ryzyka, 29 stycznia 2020 r. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

każdego z obszarów ryzyka wskazanych w unijnej skoordynowanej ocenie ryzyka w zestawie narzędzi przewidziano **plany ograniczania ryzyka** oparte na środkach o najwyższej skuteczności.

W planach tych – zgodnie z zaleceniami płynącymi z konkluzji dotyczących unijnego zestawu narzędzi uzgodnionymi przez grupę współpracy ds. bezpieczeństwa sieci i informacji – przewidziano szereg **kluczowych środków**, które mają zostać wprowadzone przez wszystkie państwa członkowskie i Komisję zgodnie z poniższym:

Konkluzje dotyczące unijnego zestawu narzędzi

W unijnym zestawie narzędzi określono szereg środków i działań, które – jeżeli zostaną odpowiednio połączone i skutecznie wdrożone – stanowić będą podstawę skoordynowanego podejścia w tej dziedzinie. W istocie, biorąc pod uwagę szeroki zakres obszarów ryzyka wskazanych w unijnej skoordynowanej ocenie ryzyka i ich zróżnicowany charakter, nie wystarczy zastosowanie wyłącznie jednego rodzaju działań, konieczne natomiast będzie wprowadzenie szeregu środków stosowanych w odpowiedniej kombinacji, aby móc skutecznie reagować na wszystkie kluczowe zagrożenia.

W oparciu o ocenę możliwych planów ograniczania ryzyka i identyfikację środków o najwyższej skuteczności we wspomnianym zestawie narzędzi zalecono, co następuje:

1. Wszystkie państwa członkowskie powinny zapewnić wprowadzenie środków (w tym nadanie organom krajowym odpowiednich uprawnień), aby zagwarantować odpowiednią i proporcjonalną reakcję na obecnie zidentyfikowane i przyszłe zagrożenia, a w szczególności zadbać o to, by były w stanie w stanie wprowadzać ograniczenia, zakazy lub określone wymogi lub warunki, zgodnie z podejściem opartym na analizie ryzyka, w odniesieniu do dostaw, wdrożenia i eksploatacji sprzętu na potrzeby sieci 5G w oparciu o szereg przesłanek związanych z bezpieczeństwem.

Państwa członkowskie powinny w szczególności:

- *zaostrzyć **wymogi w zakresie bezpieczeństwa** w odniesieniu do operatorów sieci ruchomych (np. rygorystyczne kontrole dostępu, przepisy dotyczące bezpiecznej eksploatacji i nadzoru, ograniczenia w zakresie outsourcingu konkretnych funkcji itp.);*

- *oceniać profil ryzyka dostawców, a w związku z tym **stosować odpowiednie ograniczenia w odniesieniu do dostawców uznawanych za stwarzających wysokie ryzyko – w tym niezbędne wyłączenia umożliwiające skuteczne ograniczanie ryzyka – w odniesieniu do kluczowych aktywów** wskazanych jako krytyczne i wrażliwe w unijnej skoordynowanej ocenie ryzyka (np. funkcje sieci szkieletowej, funkcje zarządzania siecią i organizacji sieci czy też funkcje sieci dostępowej);*

- *zapewniać, aby każdy operator posiadał odpowiednią strategię przewidującą korzystanie z usług wielu dostawców w celu **uniknięcia lub ograniczenia istotnego uzależnienia** od jednego dostawcy (lub dostawców o podobnym profilu ryzyka), zapewnienia odpowiedniej równowagi dostawców na szczeblu krajowym oraz **uniknięcia uzależnienia od dostawców uznanych za stwarzających wysokie ryzyko**; wymaga to również unikania sytuacji, w których występuje uzależnienie od jednego dostawcy, w tym poprzez promowanie większej interoperacyjności urządzeń.*

2. Komisja Europejska, wraz z państwami członkowskimi, powinna przyczyniać się do:

 utrzymania ***zróżnicowanego i zrównoważonego łańcucha dostaw 5G*** *w celu uniknięcia długotrwałego uzależnienia od konkretnych dostawców, w tym poprzez:*

o pełne wykorzystanie istniejących narzędzi i instrumentów UE, w szczególności monitorowanie potencjalnych ***bezpośrednich inwestycji zagranicznych*** *mających wpływ na kluczowe aktywa 5G oraz poprzez unikanie* ***zakłóceń*** *na rynku dostaw 5G wynikających z potencjalnego dumpingu lub potencjalnych subsydiów; oraz*

o dalsze zwiększanie ***zdolności UE w zakresie technologii 5G i technologii będących następcą 5G*** *poprzez wykorzystanie odpowiednich programów i środków finansowych UE;*

 ułatwienia koordynacji między państwami członkowskimi w zakresie ***normalizacji*** *w celu osiągnięcia określonych celów z zakresu bezpieczeństwa oraz opracowania* ***odpowiednich dla całej UE systemów certyfikacji*** *w celu promowania bezpieczniejszych produktów i procesów.*

3. W celu zapewnienia, by takie skoordynowane podejście wytrzymało próbę czasu, należy rozszerzyć mandat grupy roboczej w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji oraz rozbudować współpracę z innymi właściwymi organami i podmiotami w szczególności w celu:

 przeprowadzania okresowego przeglądu – przy wsparciu Komisji i ENISA – ***krajowych i unijnych ocen ryzyka*** *dotyczących bezpieczeństwa sieci 5G i sieci opartych na technologii będącej następcą 5G, dalszego opracowywania i ujednolicania stosowanej metodyki oceny oraz dostosowywania się do zmieniającej się technologii 5G;*

 prowadzenia szczegółowego i regularnego ***monitorowania i oceny wdrażania*** *zestawu narzędzi na podstawie ustrukturyzowanych sprawozdań składanych przez państwa członkowskie;*

 koordynowania i wspierania realizacji ***działań wspierających****, które wymagają współpracy na szczeblu UE, w szczególności w odniesieniu do opracowywania wytycznych i wymiany najlepszych praktyk na temat różnych środków;*

 wspierania, w stosownych przypadkach, dalszej możliwej koordynacji działań na szczeblu UE w szczególności w celu zapewnienia dalszego ujednolicania ***wymogów bezpieczeństwa technicznego i organizacyjnego dla operatorów sieci****.*

Źródło: Unijny zestaw narzędzi

Z konkluzji dotyczących zestawu narzędzi wynika, że państwa członkowskie przejawiają zdecydowaną wolę wspólnego reagowania na wyzwania związane z bezpieczeństwem sieci 5G. Ma to zasadnicze znaczenie dla bezpieczeństwa w państwach członkowskich i w całej UE, dla gospodarek krajowych, a także dla rynku wewnętrznego UE i suwerenności technologicznej Europy. Zarówno unijna skoordynowana ocena ryzyka, jak i unijny zestaw narzędzi wskazują na wysoką wartość wspólnych prac prowadzonych w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji, przy intensywnej współpracy między przedstawicielami wszystkich państw członkowskich, Komisją i ENISA.

Zestaw narzędzi umożliwia stosowanie wspólnego unijnego podejścia do cyberbezpieczeństwa sieci 5G, wspierając spójność rozwiązań na całym rynku wewnętrznym za pośrednictwem polityki UE i koordynacji działań na szczeblu Unii, a także gwarantuje państwom członkowskim wykonywanie ich kompetencji, zwłaszcza w odniesieniu do bezpieczeństwa narodowego. Zawarte w zestawie narzędzi środki ograniczające ryzyko i plany ograniczania ryzyka umożliwiają odpowiednie, skuteczne i proporcjonalne działania UE w odpowiedzi na wspólne wyzwania w zakresie cyberbezpieczeństwa sieci 5G.

Komisja z zadowoleniem przyjmuje publikację unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G i w pełni popiera wszystkie powyższe ustalenia.

Komisja wzywa państwa członkowskie oraz odpowiednie instytucje, agencje i inne organy Unii do:

(i) zapewnienia szybkiego wdrożenia skutecznych i odpowiednich strategii ograniczania ryzyka w całej UE zgodnie z unijnym zestawem narzędzi, oraz

(ii) podjęcia wszelkich niezbędnych dalszych kroków w celu zapewnienia koordynacji na szczeblu Unii, w tym poprzez kontynuowanie prac w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji oraz ustanowienie skutecznego mechanizmu monitorowania wdrażania unijnego zestawu narzędzi, aby zagwarantować skuteczność środków i sprawne funkcjonowanie rynku wewnętrznego.

5. Wdrażanie zestawu narzędzi

Zdeterminowana postawa państw członkowskich, by w pełni wykorzystywać zestaw narzędzi, ma zasadnicze znaczenie dla wiarygodnego i skutecznego europejskiego podejścia do bezpieczeństwa sieci 5G. Chociaż to państwa członkowskie będą decydować, czy dany środek jest odpowiedni w zależności od uwarunkowań krajowych, należy bezwzględnie zadbać o to, by **zestaw kluczowych środków, zaleconych przez grupę współpracy ds. bezpieczeństwa sieci i informacji (zob. konkluzje dotyczące zestawu narzędzi powyżej), został wprowadzony w każdym państwie członkowskim oraz – w odniesieniu do niektórych środków – na szczeblu UE** w celu wyeliminowania zidentyfikowanych czynników ryzyka.

Komisja jest gotowa nadal udzielać pełnego wsparcia w kolejnych fazach tego procesu i wzywa państwa członkowskie do:

- podjęcia, **do dnia 30 kwietnia 2020 r.**, konkretnych i wymiernych działań w celu wdrożenia zestawu kluczowych środków zalecanych w konkluzjach dotyczących unijnego zestawu narzędzi;

- przygotowania, **do dnia 30 czerwca 2020 r.**, sprawozdania grupy współpracy ds. bezpieczeństwa sieci i informacji na temat stanu wdrożenia tych kluczowych środków w każdym państwie członkowskim, w oparciu o regularne sprawozdania i monitorowanie prowadzone w szczególności w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji, przy wsparciu Komisji i ENISA.

5.1. Oparte na analizie ryzyka skoordynowane podejście do dostawców sprzętu 5G

Biorąc pod uwagę ostateczny cel, jakim jest zapewnienie bezpieczeństwa i odporności sieci 5G oraz ich zrównoważonego charakteru, państwa członkowskie zgodziły się co do

konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w zestawie narzędzi. Komisja jest gotowa wspierać państwa członkowskie we wdrażaniu tych środków.

Wsparciem we wdrażaniu wspomnianych środków w całej UE służą wytyczne, które zawarto w unijnej skoordynowanej ocenie ryzyka i unijnym zestawie narzędzi, dotyczące (1) oceny profilu ryzyka dostawców[17] oraz (2) wrażliwości elementów sieci i funkcji sieciowych[18], a także innych aktywów. Zarówno unijna skoordynowana ocena ryzyka, jak i środki zawarte w zestawie narzędzi dotyczą ryzyka związanego z dostawcami urządzeń i usług sieciowych 5G. Nie obejmują one innych produktów lub usług, które mogą oferować ci lub inni dostawcy.

Zgodnie z pkt 2.37 unijnej skoordynowanej oceny ryzyka profile ryzyka poszczególnych dostawców można ocenić w oparciu o szereg czynników.

Ocena profili ryzyka dostawców powinna być przeprowadzana wyłącznie w oparciu o przesłanki bezpieczeństwa i na podstawie obiektywnych kryteriów. Aby ułatwić skoordynowane podejście do wdrażania tych środków, w zestawie narzędzi zalecono, by państwa członkowskie wymieniały się informacjami na temat krajowego podejścia i najlepszych praktyk. Ponadto zdaniem Komisji działanie to powinno być jednym z pierwszych priorytetów kolejnego etapu prac w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji, przy współpracy z Komisją i ENISA.

Istotne jest, by ograniczenia dotyczące dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędne wyłączenia w celu skutecznego ograniczania ryzyka, jak również środki mające na celu uniknięcie uzależnienia od tych dostawców, stosowano na odpowiednio wczesnym etapie. Wprowadzanie tych środków na jak najwcześniejszym etapie, w tym, w miarę możliwości, w kontekście procedur wydawania pozwoleń na częstotliwości 5G, zwiększy również przewidywalność dla podmiotów gospodarczych, przyczyniając się tym samym do szybkiego uruchomienia sieci 5G, i zapewni długoterminowe bezpieczeństwo sieci 5G oraz odporność łańcucha dostaw 5G.

Jednocześnie wdrażanie tych środków na szczeblu krajowym może przebiegać według odmiennego harmonogramu, w przypadku gdy jest to konieczne i uzasadnione, w szczególności w razie wysokiego stopnia uzależnienia od sprzętu lub usług dostawców uznanych za stwarzających wysokie ryzyko (np. poprzez uwzględnienie cykli modernizacji sprzętu, w szczególności przejścia z „niesamodzielnych" na „samodzielne" sieci 5G). Państwa członkowskie mogłyby rozważyć takie zdefiniowanie planów wdrożenia, aby przewidzieć w nich odpowiednie okresy przejściowe dla operatorów sieci, których to dotyczy. W tym kontekście okresy przejściowe należy określić w taki sposób, aby utrzymać, a nawet zwiększyć zachęty do inwestowania w nowoczesne urządzenia sieciowe, w tym przyspieszyć wdrażanie pełnoprawnych („samodzielnych") sieci szkieletowych 5G i zastępowanie

[17] Pkt 2.37 unijnej skoordynowanej oceny ryzyka.

[18] W pkt 2.21 unijnej skoordynowanej oceny ryzyka przedstawiono główne kategorie elementów i funkcji oraz ich ogólny poziom wrażliwości, a także wymieniono szereg kluczowych elementów wskazanych przez państwa członkowskie dla każdej kategorii, a w pkt 2.28 i 2.29 wskazano szereg innych rodzajów wrażliwych aktywów lub obszarów (np. określone podmioty lub obszary geograficzne).

istniejących urządzeń 4G w innych częściach sieci (np. w sieciach dostępu radiowego), zgodnie z celami planu działania w zakresie sieci 5G[19].

Ponadto ze względu na złożoność sieci 5G opierających się na oprogramowaniu operatorzy telekomunikacyjni mogą w coraz większym stopniu powierzać podmiotom zewnętrznym – oprócz dostaw urządzeń sieciowych – realizację określonych zadań, takich jak utrzymanie i modernizacja sieci oraz aktualizacja oprogramowania 5G, czy też zlecać im na zasadzie outsourcingu inne usługi zarządzane. Jak opisano w unijnej skoordynowanej ocenie ryzyka, zjawisko to stanowi źródło poważnego zagrożenia dla bezpieczeństwa. W związku z tym temu aspektowi należy poświęcić szczególną uwagę. Istotne jest również przeprowadzanie szczegółowej oceny bezpieczeństwa w odniesieniu do profilu ryzyka dostawców, którym powierzono realizację tych usług, w szczególności wówczas, gdy rzeczone zadania nie są realizowane na terenie UE. W celu zachowania długoterminowej integralności infrastruktury 5G należy stosować odpowiednie środki, w tym w szczególności nakładać ograniczenia we wrażliwych obszarach sieci 5G bądź dokonywać niezbędnego wykluczenia podmiotów wysokiego ryzyka stosownie do środków ograniczających ryzyko przewidzianych w zestawie narzędzi.

5.2. Rola Komisji we wspieraniu wdrażania zestawu narzędzi

Komisja będzie nadal ogólnie wspierać wdrażanie unijnego podejścia do cyberbezpieczeństwa 5G, a także podejmować konkretne inicjatywy w odniesieniu do środków i celów przewidzianych w zestawie narzędzi, w przypadku gdy jej działania mogą wnieść wartość dodaną. Komisja będzie w pełni korzystać ze swoich kompetencji i odpowiednich instrumentów w zakresie niezbędnym do wyeliminowania problemów związanych z bezpieczeństwem. W ten sposób, działając wspólnie z państwami członkowskimi i sektorem prywatnym, Komisja dąży do wspierania strategicznych środków, które przyczynią się do zapewnienia suwerenności technologicznej UE i jej wiodącej roli w procesie dalszego rozwoju technologii sieciowych, technologii z zakresu cyberbezpieczeństwa i wszystkich istotnych elementów składowych, od których zależą nasza cała gospodarka i nasze bezpieczeństwo.

W szczególności Komisja podejmie następujące działania w celu zapewnienia wdrożenia odpowiednich środków ograniczających ryzyko zawartych w zestawie narzędzi w obszarach wchodzących w zakres jej kompetencji:

Zapewnienie cyberbezpieczeństwa sieci 5G i zdywersyfikowanego łańcucha wartości 5G:

- **współpraca w dziedzinie cyberbezpieczeństwa**: zapewnienie państwom członkowskim dalszego wsparcia w skutecznym, skoordynowanym i terminowym wdrażaniu środków krajowych za pośrednictwem grupy współpracy ds. bezpieczeństwa sieci i informacji;

- **przepisy dotyczące telekomunikacji i cyberbezpieczeństwa**: zapewnianie wsparcia we wdrażaniu środków (przewidzianych w zestawie narzędzi) dotyczących wymogów w zakresie bezpieczeństwa, w szczególności w odniesieniu do odpowiednich przepisów w ramach europejskich przepisów dotyczących łączności elektronicznej, oraz rozważenie wartości dodanej ewentualnych aktów wykonawczych określających szczegółowo techniczne

[19] COM(2016) 588 z dnia 14 września 2016 r., „Sieć 5G dla Europy: plan działania”.

i organizacyjne środki bezpieczeństwa w celu uzupełnienia przepisów krajowych oraz zwiększenia skuteczności i spójności środków bezpieczeństwa nakładanych na operatorów;

- **normalizacja**: podjęcie działań mających na celu utrzymanie i w razie potrzeby zwiększenie udziału Europy w odpowiednich organach normalizacyjnych, aby osiągnąć cele Europy w zakresie bezpieczeństwa i interoperacyjności. W szczególności Komisja wraz z państwami członkowskimi będzie oceniać i propagować specyfikacje i normy techniczne umożliwiające interoperacyjność między dostawcami urządzeń 5G w różnych częściach sieci, w tym w dotychczasowych sieciach, aby stworzyć otoczenie autentycznie sprzyjające współistnieniu wielu dostawców, na przykład poprzez otwarte i interoperacyjne interfejsy;

- **certyfikacja**: wspieranie rozwoju systemów certyfikacji 5G uwzględniających potrzeby sieci 5G w oparciu o unijne ramy certyfikacji cyberbezpieczeństwa;

- **monitorowanie bezpośrednich inwestycji zagranicznych**: wspieranie wdrażania unijnych ram monitorowania poprzez mapowanie łańcucha wartości sieci 5G, w tym wrażliwych aktywów sieciowych, oraz regularne monitorowanie bezpośrednich inwestycji zagranicznych w całym łańcuchu wartości. Zgodnie z harmonogramem monitorowania bezpośrednich inwestycji zagranicznych (począwszy od października 2020 r.) Komisja będzie kontrolować inwestycje zagraniczne w obszarze 5G według wytycznych zawartych w rozporządzeniu (UE) 2019/452, z uwzględnieniem unijnej skoordynowanej oceny ryzyka i unijnego zestawu narzędzi;

- **instrumenty ochrony handlu**: monitorowanie wszystkich istotnych zmian na rynku w UE i w państwach trzecich oraz ochrona unijnych podmiotów na europejskim rynku 5G za pomocą środków ochrony handlu w celu zaradzenia ewentualnym praktykom zakłócającym handel (dumping lub subsydiowanie), w tym poprzez wszczynanie, w stosownych przypadkach, wstępnych postępowań wyjaśniających;

- **reguły konkurencji:** monitorowanie funkcjonowania rynków dostaw sprzętu i oprogramowania 5G, aby zadbać o to, by gwarantowały konkurencyjność, w tym w odniesieniu do możliwych sytuacji uzależnienia się od jednego dostawcy w oparciu o warunki umowy lub pod względem technologicznym;

- **unijne programy finansowania**: zapewnienie, aby uczestnictwo w unijnych programach finansowania w odpowiednich dziedzinach technologii było uzależnione od spełnienia wymogów w zakresie bezpieczeństwa, poprzez pełne wykorzystanie i dalsze wdrażanie warunków bezpieczeństwa w programach w zakresie badań naukowych i innowacji, w szczególności w programie „Horyzont Europa", programie „Cyfrowa Europa" i instrumencie „Łącząc Europę 2", w europejskich funduszach strukturalnych i inwestycyjnych oraz w innych odpowiednich programach. Podobne podejście należy przyjąć również w unijnych zewnętrznych programach finansowania i instrumentach finansowych UE, w tym w odniesieniu do finansowania zapewnianego przez międzynarodowe instytucje finansowe;

- **zamówienia publiczne:** wykorzystanie zamówień publicznych w obszarze sieci 5G w celu wspierania określonych celów z zakresu bezpieczeństwa, różnorodności dostawców i długoterminowej stabilności sieci 5G; w szczególności dążenie do zapewnienia należytego uwzględnienia aspektów bezpieczeństwa przy udzielaniu zamówień publicznych związanych z obszarem sieci 5G, zgodnie z unijnymi przepisami dotyczącymi zamówień publicznych;

- **reagowanie na incydenty i zarządzanie kryzysowe (plan działania) i ćwiczenia w dziedzinie cyberbezpieczeństwa**: pełne stosowanie unijnego planu[20] skoordynowanego reagowania na cyberincydenty na dużą skalę. Ponadto Komisja, wraz z ENISA, rozważy możliwość przeprowadzenia ćwiczenia w dziedzinie cyberbezpieczeństwa w sieciach 5G, gdy tylko pozwoli na to dojrzałość rynku.

Ponadto pod kierunkiem Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa i Wiceprzewodniczącego Komisji oraz Rady:

- **ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne (zestaw narzędzi dla dyplomacji cyfrowej)[21]**: w przypadku szkodliwych działań w cyberprzestrzeni, które zagrażają integralności i bezpieczeństwu UE, zachęca się państwa członkowskie do stosowania odpowiednich środków wspólnej polityki zagranicznej i bezpieczeństwa w ramach unijnego zestawu narzędzi dla dyplomacji cyfrowej (w tym, w razie konieczności, środków ograniczających) w celu promowania współpracy, ułatwiania łagodzenia zagrożeń i wywierania wpływu na zachowania potencjalnych agresorów.

Ponadto do osiągnięcia celu, jakim jest uniknięcie lub ograniczenie ryzyka długotrwałej zależności, przyczyni się szereg programów promujących zróżnicowany i zrównoważony rynek 5G, w tym poprzez utrzymanie zdolności UE w łańcuchu wartości 5G oraz inwestowanie w innowacje, zgodnie z międzynarodowymi zobowiązaniami UE.

Promowanie innowacji oraz inwestowanie w cyberbezpieczeństwo i technologie z zakresu infrastruktury sieciowej:

- **unijne programy finansowania**: zwiększenie inwestycji w badania naukowe, innowacje i wdrażanie technologii sieciowych i podstawowe elementy składowe sieci. W ramach następnego budżetu UE na lata 2021–27 Komisja zaproponowała blisko 3 mld EUR na inwestycje w technologie w dziedzinie cyberbezpieczeństwa. Obejmuje to badania naukowe i innowacje w ramach programu „Horyzont Europa" oraz wsparcie zdolności w zakresie cyberbezpieczeństwa w ramach programu „Cyfrowa Europa". Program InvestEU może również udzielać wsparcia finansowego na badania i rozwój w obszarze 5G, a także wsparcia dla wdrażania tej technologii.

Ponadto w ramach kolejnego programu „Horyzont Europa"[22] Komisja zaproponowała utworzenie zinstytucjonalizowanego partnerstwa UE w sprawie NGI/6G („inteligentne sieci i usługi"), we współpracy z przemysłem i w koordynacji z państwami członkowskimi, w celu ukończenia wdrażania technologii 5G, a przede wszystkim w celu **poczynienia przygotowań pod kątem 6G**, czyli technologii mobilnej kolejnej generacji. W budżecie UE (na lata 2021–27) na potrzeby tej inicjatywy przewidziano inwestycje UE na kwotę ponad 2,5 mld EUR, którym towarzyszyć mają inwestycje sektora prywatnego na kwotę co najmniej 7,5 mld EUR.

[20] Zalecenie Komisji (UE) 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.
[21] Konkluzje Rady z dnia 20 listopada 2017 r., 9916/17.
[22] Finansowanie może być również udostępniane za pośrednictwem instrumentu „Łącząc Europę 2.0" i programu „Cyfrowa Europa".

- **opracowywanie i wdrażanie projektów przemysłowych**: dokonanie oceny potencjalnych luk lub braków na rynku w łańcuchu wartości 5G, które uzasadniałyby ukierunkowane działania w ramach następnego długoterminowego budżetu lub ewentualnych projektów IPCEI (ważne projekty stanowiące przedmiot wspólnego europejskiego zainteresowania) w dziedzinie cyberbezpieczeństwa, zgodnie z sugestiami forum wysokiego szczebla ds. IPCEI. Decyzja o opracowaniu i zainicjowaniu projektów IPCEI leży w gestii państw członkowskich i przedsiębiorstw. Przepisy UE przewidują ramy sprzyjające realizacji tego typu projektów, a Komisja jest gotowa ułatwić niezbędne kontakty i udzielić wytycznych.

6. Wnioski

Sieci 5G mają zapewnić szereg możliwości obywatelom, społeczeństwom i gospodarce w Europie. Zapewnienie bezpieczeństwa i odporności sieci 5G ma zatem kluczowe znaczenie. Jednocześnie zagrożenia dla cyberbezpieczeństwa (w tym ryzyko ingerencji ze strony państw spoza UE lub podmiotów wspieranych przez państwa obce) stanowią coraz większe wyzwanie, które staje się coraz istotniejsze wraz z coraz większym uzależnieniem od technologii i danych. Zaniedbywanie cyberbezpieczeństwa może podważyć zaufanie do rozwoju gospodarki cyfrowej i społeczeństwa cyfrowego i uniemożliwić UE czerpanie pełni związanych z tym korzyści. Wymaga to bardziej stanowczych reakcji, odpowiednio dostosowywanych do zmieniających się okoliczności.

Skoordynowane i spójne podejście do cyberbezpieczeństwa w UE w odniesieniu do kluczowych technologii i sieci ma zasadnicze znaczenie dla UE, aby zapewnić jej suwerenność technologiczną oraz utrzymanie i rozwój potencjału przemysłowego. Komisja będzie w pełni wspierać wdrażanie unijnego podejścia do cyberbezpieczeństwa sieci 5G, a jednocześnie zadba o to, by rynki UE pozostawały otwarte na produkty i usługi, które będą zgodne ze zmieniającymi się wymogami w zakresie cyberbezpieczeństwa i zaufania.

W tym celu ważne jest niesłabnące zaangażowanie wszystkich zainteresowanych stron na rzecz bezpieczeństwa 5G, które wymagać będzie stałej współpracy między państwami członkowskimi, Komisją i ENISA.

Komisja wzywa państwa członkowskie do podjęcia – jako kolejnego kroku, jak wskazano powyżej – szybkich działań w celu skutecznego i obiektywnego wdrożenia środków uzgodnionych w ramach zestawu narzędzi oraz do kontynuowania współpracy, przy wsparciu Komisji i ENISA, w celu zapewnienia koordynacji na szczeblu UE. Równocześnie Komisja zainicjuje wszelkie istotne działania w ramach swoich kompetencji, aby wspierać wdrażanie zestawu narzędzi przez państwa członkowskie i zwiększyć jego skuteczność .

Załącznik: Kategorie ryzyka (źródło: Unijna skoordynowana ocena ryzyka).

	Kategorie ryzyka
Scenariusze ryzyka związane z niewystarczającymi środkami bezpieczeństwa	*R1: Niewłaściwa konfiguracja sieci*
	R2: Brak kontroli dostępu
Scenariusze ryzyka związane z łańcuchem dostaw 5G	*R3: Niska jakość produktu*
	R4: Zależność od pojedynczego dostawcy w obrębie poszczególnych sieci lub brak różnorodności w skali kraju
Scenariusze ryzyka związane ze sposobem działania głównych agresorów	*R5: Ingerencja państwa za pośrednictwem łańcucha dostaw 5G*
	R6: Wykorzystanie sieci 5G przez zorganizowaną przestępczość lub organizacja przestępcza atakująca użytkowników końcowych
Scenariusze ryzyka związane ze współzależnościami między sieciami 5G a innymi systemami krytycznymi	*R7: Znaczące zakłócenie funkcjonowania infrastruktury krytycznej lub usług krytycznych*
	R8: Wielka awaria sieci spowodowana przerwaniem dostaw energii elektrycznej lub innych systemów wspierających
Scenariusze ryzyka związane z urządzeniami użytkowników końcowych	*R9: Wykorzystywanie internetu rzeczy w złych zamiarach*