PIIT

Warszawa, dnia 14 sierpnia 2019
PIIT1309/19

Pan Minister
Marek Zagórski

Ministerstwo Cyfryzacji

Szanowny Panie Ministrze!

Polska Izba Informatyki i Telekomunikacji (PIIT) w załączeniu przekazuje Opinię do projektu uchwały Rady Ministrów ws Strategii Cyberbezpieczeństwa RP na lata 2019-2024, z prośbą o uwzględnienie w dalszych pracach Ministerstwa.

Łączę wyrazy szacunku.

Załączniki 2:

-Opinia PIIT (str. 12)

-Opinia PIIT z dn. 01.07.2019

Andrzej Dulka
Prezes PIIT

26 PIIT lat
Polska Izba Informatyki i Telekomunikacji
Eurocentrum Alfa, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 691 119 555
fax: +48 22 628 55 36
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A. Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. m.st. W-wy
XII Wydział Gospodarczy

Opinia Polskiej Izby Informatyki i Telekomunikacji (PIIT)
do projektu uchwały Rady Ministrów ws Strategii Cyberbezpieczeństwa RP na lata 2019-2024

UWAGI OGÓLNE

W pierwszej kolejności, jako organizacja zrzeszająca kluczowe podmioty rynku telekomunikacyjnego i teleinformatycznego chcielibyśmy podkreślić, że kwestie cyberbezpieczeństwa traktujemy z najwyższą uwagą. Szczególnie w obliczu zwiększającego się udziału technik cyfrowych zarówno w życiu prywatnym, gospodarczym, jak i funkcjonowaniu administracji publicznej uważamy, że obszar ten będzie kluczowy dla faktycznego osiągnięcia pozytywnych skutków, jakie zazwyczaj wiąże się z cyfryzacją, w tym wzrostu innowacyjności, pobudzenia gospodarczego, w tym wzrostu PKB, czy zmian na rynku pracy. Skuteczne zaadresowanie kluczowych wyzwań będzie przy tym istotne z punktu widzenia całości cyfrowego ekosystemu i wszystkich jego uczestników.

Uwaga ogólna 1. Strategia Cyberbezpieczeństwa a Krajowe Ramy Polityki Cyberbezpieczeństwa
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 ma zastąpić Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017 – 2022 przyjęte uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.
Z porównania obydwu dokumentów wynika, że do proponowanego obecnie projektu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, zwanej dalej Strategią, dodany został jeden cel szczegółowy: „Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa". Warto dodać, że już w dokumencie rządowym „Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia" z 2009 roku jednym z 3 filarów działań, poza działaniami organizacyjno-prawnymi i działaniami technicznymi miała być „Edukacja społeczna i specjalistyczna". Cieszy, że przywraca się rangę tego zagadnienia po latach.
Dokument projektu Strategii wydaje się być adaptacją poprzedniego dokumentu Krajowych Ram Polityki Cyberbezpieczeństwa jest więc wynikiem pewnej ewolucyjnej a nie gwałtownej zmiany. Niestety, nie operuje wysokością środków finansowych oraz ilościowymi miernikami stawianych celów. Istnieje zatem ryzyko, że dokument w niewielkim stopniu może wpłynąć na poprawę poziomu bezpieczeństwa cybernetycznego. Patrz także uwagi ogólne 4 i 5.

Uwaga ogólna 2. Potrzebna jest uszczegółowiona diagnoza i podsumowanie dotychczasowych działań
W dokumentach strategicznych, przyjmowanych na poziomie Rady Ministrów jednym z kluczowych elementów jest przygotowanie diagnozy aktualnego stanu spraw, do którego odnosi się dany dokument. Tymczasem w skierowanym do konsultacji dokumencie element ten nie został wystarczająco przedstawiony.
Sugerujemy więc zwięzłe, obiektywne omówienie aktualnego stanu systemu cyberbezpieczeństwa oraz warunków funkcjonowania cyberprzestrzeni, wskazanie słabości i deficytów, których niwelowanie będzie jednym z celów działań w najbliższych latach, a także mocnych stron i atutów, jakie cechują obecną sytuację, których wzmocnienie i rozbudowa w przyszłości pozwoli realizować cele strategii. Dopiero dysponując taką bazą wyjściową, w postaci swoistej "fotografii" aktualnego stanu, pozwoli to w zrozumiały sposób opisać zamierzenia, jakie państwo polskie stawia przed sobą oraz wskazać środki, metody, formy ich osiągania, przewidziane przez rząd.
W naszej ocenie należy przeprowadzić i przedstawić analizę pod kątem m.in.:

- efektów dotychczasowych strategii i planów w zakresie cyberbezpieczeństwa;

- efektów dotychczasowych działań legislacyjnych, w szczególności z uwzględnieniem poruszanych w projekcie ustaw o krajowym systemie cyberbezpieczeństwa oraz zarządzaniu kryzysowym;
- kluczowych interesariuszy obszaru cyberbezpieczeństwa, w tym użytkowników indywidualnych i instytucjonalnych, administracji publicznej, w tym samorządowej (np. raport NIK w tej sprawie), producentów oprogramowania i urządzeń wykorzystywanych w ekosystemie teleinformatycznym, w którym mogą wystąpić zagrożenia cyberbezpieczeństwa, dostawców usług świadczonych za pośrednictwem sieci internet, dostawców usług szerokopasmowych, cyberprzestępców, służb, policji, prokuratury, oraz sądów.

Uwaga ogólna 3. Strategia Cyberbezpieczeństwa a ogólna polityka bezpieczeństwa
Należy podkreślić, że nie można oderwać Strategii Cyberbezpieczeństwa od ogólnej polityki bezpieczeństwa narodowego realizowanej przez Rzeczpospolitą. Kształtowanie programów cyberbezpieczeństwa musi być przygotowane w relacji do sojuszy i relacji międzynarodowych naszego kraju (NATO, Unia Europejska, relacje bilateralne).
Istotną przesłanką, wymagającą uwzględnienia w strategii, jest pojawienie się nowego podejścia do kształtowania polityki zagranicznej państw dysponujących zaawansowaną technologią informatyczną. Kontrola dostępu do kluczowych elementów technologii może być wykorzystywana do kształtowania relacji międzypaństwowych (Chiny – technologia 5G, USA – systemy operacyjne), a przez to kształtowania bezpieczeństwa gospodarczego innych krajów, znacznie wykraczającego poza cyberprzestrzeń. Z tego powodu zagadnienie bezpieczeństwa w cyberprzestrzeni nabiera dodatkowego, nieznanego dotąd wymiaru - tj. dostępu do kluczowych technologii informatycznych.
Element prowadzenia polityki zagranicznej przy pomocy reglamentowania dostępu do kluczowych technologii informatycznych może w określonym zakresie wpływać na krajową politykę prowadzenia prac badawczo-rozwojowych. Podstawą do opracowania tematyki badań powinien być przeprowadzony audyt technologii wykorzystywanych przez instytucje państwowe. Audyt powinien wskazać jakie technologie mają zastosowanie w poszczególnych obszarach (obronność, energetyka, finanse, służba zdrowia itp.) oraz jakie jest ryzyko związane z wystąpieniem ograniczenia dostępu do technologii z powodu występującej w danym roku sytuacji geopolitycznej. Audyt taki powinien być prowadzony raz do roku.

W wyniku przeprowadzonego audytu powinny być typowane rozwiązania technologiczne, których pozyskanie w toku prac badawczo-rozwojowych jest istotne z punktu istotnego interesu bezpieczeństwa państwa, pomimo tego, że pozyskane rozwiązanie nie jest rozwiązaniem innowacyjnym na skalę światową i jest w zasięgu możliwości naszego kraju. Elementem ważniejszym od samej innowacyjności powinno być zapewnienie możliwie jak najwyższej i uzasadnionej ekonomicznie suwerenności cyfrowej.

Uwaga ogólna 4. Kryteria sukcesu
Podstawowe zastrzeżenie względem dokumentu polega także na tym, że projekt Strategii nie ustala żadnych zobowiązań i mierników pozwalających ocenić sukces jej wdrożenia. Zarazem projekt Strategii nie zawiera żadnych wyraźnie wskazanych środków finansowych do wydatkowania przez państwo na cyberbezpieczeństwo. Strategia powinna stawiać sobie pewne cele, które mierzalnie można ocenić, na przykład „w 2024 roku wszystkie / 90% samorządów będą miały wsparcie / zapewniony kontakt ze specjalistami zajmującymi się obsługą incydentów teleinformatycznych i państwo będzie to finansować.” Albo: „do roku 2024 państwo przeznaczy minimum 200 mln złotych na otwieranie i rozwinięcie nowych kierunków studiów na uczelniach państwowych zajmujących się kształceniem

specjalistów od cyberbezpieczeństwa". W dokumencie nie znajdzie się takich zobowiązań, nie znajdzie się minimalnych progów wydatkowania środków, które ułatwiłyby przy planowaniu budżetu zarezerwowanie takich środków w budżetach poszczególnych ministerstw i instytucji.

Uwaga ogólna 5. Brak określenia sposobu finansowania zadań i oceny skutków finansowych
Sygnalizujemy, że w projekcie strategii nie zostały określone koszty jej wdrożenia oraz źródła pokrycia tych kosztów. Z jednej strony dokument strategiczny o charakterze wdrożeniowym powinien przewidywać zakres obciążenia budżetu państwa wobec działań koniecznych do wykonywania po stronie organów administracji publicznej. Z drugiej natomiast strony, mając niewątpliwy wpływ na gospodarkę i przedsiębiorców powinien przynajmniej szacować te koszty i oceniać wpływ na dotychczasowe prowadzenie działalności gospodarczej. Taka ocena powinna zostać dokonana przynajmniej szacunkowo lub kierunkowo, jeśli szczegółowe rozwiązania nie są jeszcze znane i zostaną przygotowane dopiero na etapie prac legislacyjnych. Z opisanych wyżej i planowanych do wprowadzenia rozwiązań jasno bowiem wynika, że będą one wymagały podjęcia działań wdrożeniowych po stronie przedsiębiorców objętych regulacjami, a więc będą generowały koszty.
Tymczasem w projekcie OSR do strategii wskazano: „Projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców". Wskazuje to jasno, że odpowiednia analiza nie została przeprowadzona.
Jednocześnie postulujemy rozważenie możliwości stworzenia odpowiedniego funduszu albo innej formuły, w ramach której mogłyby być finansowane i wspierane wdrożenia rozwiązań cyberbezpieczeństwa w przedsiębiorstwach i samorządach. Pozwoliłoby to z jednej strony na sprawniejsze i pełniejsze wdrożenie postanowień nowych przepisów regulujących ten obszar, a z drugiej na upowszechnienie rozwiązań cyberbezpieczeństwa w podmiotach, w których z uwagi na brak dostępnego finansowania własnego, nie mogłyby one zostać wdrożone. Brak zapewnienia takiego finansowania będzie bowiem kluczową barierą dla faktycznej budowy rozwiązań zapewniających odporność sieci, usług i urządzeń na zagrożenia.
Wypunktowanie wielu zasadnych aktywności, które jednak bez wątpienia dla skutecznego przeprowadzenia wymagają niemałych środków finansowych.

Przykładowe wymienione w projekcie Strategii aktywności, które na pewno wbrew deklarowanemu, iż zapewnione są na nie środki, wymagają zarezerwowania znacznych dodatkowych środków np. dot. pkt.:

- 5.3 Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym;
- 5.4 Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej;
- 7.1 Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
- 7.2 Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa.

Bez takiego, nawet zgrubnego, określenia wielkości nakładów i zasobów (ludzie, czas, pieniądze) może okazać się, że dokument jest kolejną papierową strategią, której nie sposób wdrożyć w latach 2019-2024. Winna być wskazana przynajmniej minimalna kwota niezbędna do realizacji Strategii.
Jednocześnie wskazanie budżetu może zdecydowanie pomóc w weryfikacji wszystkich przedstawionych w Strategii działań.

Uwaga ogólna 6. Potrzeba współpracy na etapie doprecyzowania i wdrażania założeń strategii
Powyżej sygnalizowane zagadnienia uzasadniają w naszej ocenie przyjęcie modelu realizacji strategii, w którym szczegółowe rozwiązania będą opracowywane we współpracy z podmiotami, których mają dotyczyć. W tym celu utrzymana może być dotychczas stosowana dla niektórych zagadnień formuła grup roboczych lub wprowadzenie modelu uszczegółowionych konsultacji z otwartą grupą potencjalnie zainteresowanych nowymi regulacjami podmiotów.
W tym zakresie identyfikujemy przede wszystkim tematy, takie jak:

- nowe regulacje odnośnie infrastruktury krytycznej, operatorów usług kluczowych oraz usług cyfrowych;
- uruchomienie systemu teleinformatycznego wspierającego funkcjonowanie KSC;
- wydawanie zaleceń organizacyjnych i technicznych przez organy właściwe;
- wsparcie samorządów wz. kompetencji i doboru, wdrażania oraz utrzymania środków technicznych;
- standaryzacja rozwiązań zabezpieczających;
- metodyka statycznego i dynamicznego szacowania ryzyka;
- wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa;
- podjęcie i poszerzenie współdziałania organów ścigania z innymi podmiotami;
- opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa;
- utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa.

Uwaga ogólna 7. Zakres zadań sugeruje znaczną liczbę nowych obowiązków, nakładanych na ograniczony zakres podmiotów
Projekt strategii w znaczącej części poświęcony jest zapowiedzi nowych wymagań wobec operatorów usług kluczowych, usług cyfrowych, infrastruktury krytycznej czy operatorów telekomunikacyjnych. W tym zakresie wspomina się m.in. o:

- rekomendowane będą minimalne wymagania w zakresie cyberbezpieczeństwa ze szczególnym uwzględnianiem zarządzania ciągłością działania. Analogicznym reżimem objęci zostaną dostawcy usług cyfrowych;
- zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i usług kluczowych, uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego
- doprecyzowane mają zostać obowiązki dostawców usług cyfrowych
- Organy właściwe będą mogły w tym celu wydawać zalecenia organizacyjne i techniczne

Technologie informatyczne (IT) wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych), stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom. Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT). Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT, będzie traktowane przez Radę Ministrów jako priorytet. Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa.
W pierwszej kolejności, zaznaczamy, odnosimy wrażenie, że w istotnym stopniu miałoby dochodzić do zacierania granic i zakresu obowiązków pomiędzy operatorami usług kluczowych, infrastruktury

krytycznej i usług cyfrowych. Kwestia ta wymaga istotnego wyjaśnienia i doprecyzowania, szczególnie, że aktualnie są to różne zakresy opisane w różniących się niekiedy w sposób istotny reżimach prawnych.
W drugiej kolejności z rozważanych rozwiązań wyłania się obraz, w którym dominująca część dodatkowych obowiązków i odpowiedzialności spoczywa na operatorach usług kluczowych, dostawcach usług cyfrowych, operatorach infrastruktury krytycznej, w tym operatorach telekomunikacyjnych. Trudno zanegować ich istotne znaczenie, jednak należy podkreślić, że podmioty te nie są jedynymi, których działalność ma istotny wpływ na cyberbezpieczeństwa. W tym kontekście niejako poza systemem cyberbezpieczeństwa wydają się zlokalizowani, dostawcy sprzętu i urządzeń (zarówno używanych w sieciach telekomunikacyjnych, teleinformatycznych, jak i urządzeń konsumenckich) mający przecież istotną rolę w zakresie bezpieczeństwa. Taka dysproporcja jest tym bardziej widoczna, jeśli weźmiemy pod uwagę aktualnie toczącą się dyskusję o kluczowych źródłach ryzyka w obszarze bezpieczeństwa i jakości urządzeń oraz oprogramowania sieciowego, które były powodem podjęcia działań m.in. na poziomie UE odzwierciedlonych w komunikatach i Zaleceniach Komisji Europejskiej.
W naszej ocenie, adresatem nowych obowiązków i wymagań w zakresie bezpieczeństwa powinni być więc także dostawcy ww. sprzętu i oprogramowania. W tym kontekście, uwzględniając komunikowane już założenia wyrażone w stanowisku Polski przekazanym do Komisji Europejskiej w zakresie bezpieczeństwa sieci 5G, jednym z takich wymagań w kontekście potencjalnie wymaganej dywersyfikacji sprzętu uzasadniony byłby obowiązek zapewnienia wzajemnej kompatybilności i interoperacyjności.
W zakresie zagrożeń związanych z cyberbezpieczeństwem w budowie sieci 5 G Polska Izba Informatyki i Telekomunikacji przedstawiła Pełnomocnikowi Rządu d.s. Cyberbezpieczeństwa swoją ocenę ryzyk.
Opinia Polskiej Izby Informatyki i Telekomunikacji z dnia 01.07.2019 r. w sprawie Rekomendacji Komisji Europejskiej dot. Cyberbezpieczeństwa w sieci 5G Strasbourg, 26.3.2019 C(2019) 2335 final (w załączeniu).
Trudno jednocześnie ocenić przedstawione w projekcie strategii zamierzenia, ponieważ nie zostały uszczegółowione do poziomu, na którym możliwe byłoby przedstawienie merytorycznej i kompleksowej opinii. Wyłania się jednak z nich obraz, w którym w ramach przyszłych prac legislacyjnych na pewną ograniczoną grupę podmiotów zostaną nałożone nowe obowiązki, które będą musiały być spełnione pod rygorem kar administracyjnych.
Zasadnicza wadą projektu Strategii jest także to, że w nikłym stopniu odnosi się on do kluczowych zjawisk związanych z rozwojem nowoczesnych technologii i dynamicznie rozwijającym się rynkiem informatycznym w najbliższych latach takich jak:

- Rozwój Internetu Rzeczy (IOT);
- Sztuczna Inteligencji (uczenie maszynowe) (AI);
- Mobilne sieci szerokopasmowe 5 generacji (5G);
- Przemysł 4.0
- Chmura obliczeniowej;
- Megadane (Big Data);
- Telewizja i radio cyfrowe;
- Dystrybucja treści multimedialnych w Internecie,

czy przechodzeniem w sieci Internet z protokołu IPv4 na IPv6. (Kwestie te poruszono śladowo w kontekście potrzeby rozwoju badan naukowych w pkt. 7.2 Strategii).
W naszym przekonaniu, przynajmniej kilka z nich, wymaga szerszego omówienia ze względu na zagrożenia dla cyberbezpieczeństwa. Zagrożenia związane z rozwojem internetu rzeczy i rozwojem

sztucznej Inteligencji trafnie opisane zostały w dokumentach, przygotowanym wspólnie przez Ministerstwo Cyfryzacji z sektorem biznesowym i NGO w ramach Grup Roboczych powoływanych do wdrożenia Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Uwagi szczegółowe do projektu Strategii

Uwaga szczegółowa 1. Projekt określa podstawowy cel Strategii, którym jest:
„Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim odporności systemów informacyjnych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni, a także zwiększyć poziom ochrony informacji w systemach informacyjnych poprzez standaryzację zabezpieczeń. Realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni."
Czy celem nie powinien być także nie zakłócany poważnymi incydentami, rozwój Polski, w tym gospodarki i społeczeństwa, także w tych dziedzinach, które dziś nie są objęte bezpośrednio regulacjami wynikającymi z UKSC np. media, nauka i badania, kultura narodowa, rozwój MŚP etc. Co zresztą autorzy podkreślają w innej części tzn. w WIZJI (pkt 4 Strategii).

Uwaga szczegółowa 2. Zapowiadana jest zmiana regulacji prawnych w skali UE dot. chmury i dot. operatorów usług cyfrowych, ale bez wskazania kierunków tych zmian. Mowa jest jedynie o konieczności doprecyzowania obowiązków. Czy możemy wskazać najważniejsze przyczyny takiej potrzeby? Należy pamiętać także że rozwiązania chmurowe są istotna częścią technologii 5G i niezbędnym elementem rozwoju przemysłu 4.0.
Strategia proponuje:
„Zmiany przepisów regulujących funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa będą również wynikały z praktyki funkcjonowania na szczeblu europejskim Dyrektywy 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 (Dz. U. L 194 z 19.7.2016, str. 1), zwanej dalej „Dyrektywą NIS". Doświadczenia związane ze stosowaniem przepisów prawa w tym zakresie będą również przesłanką do wnioskowania na poziomie Unii Europejskiej w sprawie zmiany przepisów samej Dyrektywy NIS, tak aby zwiększyć skuteczność jej oddziaływania – jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych.
Uwaga szczegółowa 3. Zapowiadane jest wdrożenie nowego Systemu Teleinformatycznego który zgodnie z art. 46 ust.1 UKSC ma zapewnić:
„Podniesienie efektywności funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie realizowane poprzez uruchomienie w roku 2021 przez ministra właściwego do spraw informatyzacji systemu teleinformatycznego wspierającego:
1) współpracę podmiotów wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa,
2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa,
3) zgłaszanie i obsługę incydentów,
4) szacowanie ryzyka na poziomie krajowym,

5) ostrzeganie o zagrożeniach cyberbezpieczeństwa."
Wydaje się ze za generowanie rekomendacji (pkt.2) powinien odpowiadać określony podmiot a nie System Teleinformatyczny, choć można i należy zakładać, że część z nich będzie generowana automatycznie wg określonych algorytmów.

Uwaga szczegółowego 4. Czy musimy pisać w Polskiej Strategii, że będziemy ćwiczyli w ramach sił zbrojnych wyłącznie operacje defensywne?
„Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie weryfikowana podczas ćwiczeń sektorowych oraz ćwiczeń krajowych, inicjowanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa. W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia operacji defensywnych w cyberprzestrzeni".
Wydaje się ze nie powinniśmy wykluczać możliwości ćwiczenia operacji ofensywnych w przypadku odpowiedzi na agresję, a przynajmniej potencjalny agresor nie powinien czuć się bezkarny i sądzić, że jesteśmy przygotowywani, jako państwo, tylko do działań defensywnych.

Uwaga szczegółowa 5. Z pkt. 5.4 Strategii wynika ze rząd posiada już analizy dot. operatorów telekomunikacyjnych w budowie sieci 5G – chętnie byśmy się z nimi zapoznali jako środowisko firm zainteresowanych budową sieci 5G i operatorów telekomunikacyjnych, zwłaszcza że analizy te mają być podstawą do tworzenia zmian prawnych, jak wskazuje Strategia. Kierunki tych zmian powinna określać Strategia Cyberbezpieczeństwa, np. w podobny sposób jak sygnalizowała KE w komunikacie: http://europa.eu/rapid/press-release_IP-19-1832_pl.htm, w którym czytamy m.in., że: Po analizie ryzyka …"państwa członkowskie powinny zaktualizować dotychczasowe wymogi w zakresie bezpieczeństwa, którym podlegają dostawcy usług sieciowych, oraz wprowadzić warunki gwarantujące bezpieczeństwo sieci publicznych, zwłaszcza przy przyznawaniu praw użytkowania częstotliwości radiowych w pasmach 5G. Środki te powinny obejmować nałożenie na dostawców i operatorów zaostrzonych wymogów, zobowiązujących ich do zapewnienia bezpieczeństwa sieci. Krajowe oceny ryzyka oraz środki powinny uwzględniać różne czynniki ryzyka, takie jak ryzyko techniczne oraz ryzyko związane z zachowaniem dostawców lub operatorów, w tym dostawców i operatorów z państw trzecich." PIIT zwraca w szczególności uwagę na potrzebę stosowania otwartych standardów w budowie sieci 5G jako niezbędnego elementu zapewnienia cyberbezpieczeństwa w sieciach 5G.
W projekcie Strategii czytamy: „Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT). Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT, będzie traktowane przez Radę Ministrów jako priorytet. Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa".
Z zadowoleniem przyjmujemy wolę współpracy organizacjami USA i brytyjskimi dot. Operatorów usług cyfrowych co znalazło zasygnalizowane w zdaniu dot. współpracy w ramach:
„…Grupy Współpracy Dyrektywy NIS, a także w ramach współpracy transatlantyckiej z brytyjskimi i amerykańskimi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych".
Mamy nadzieje, że kontakty te będą prowadzić także do wzajemnego uznawania standardów i certyfikatów.

W związku z powyższym proponujemy też na s.13 pkt 5.4 ostatni paragraf dodać zapis: „Grupy Współpracy Dyrektywy NIS, a także w ramach współpracy z międzynarodowymi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych." Pozwoli to na uspójnienie treści z tekstem celu szczegółowego nr 5 (s. 22 pkt 9.1). Taki zapis obejmuje wszystkie instytucje i ośrodki akademickie, w tym również funkcjonujące poza Grupą Współpracy Dyrektywy NIS.

Uwaga szczegółowa 6. Metody szacowania ryzyka – czy powinna być jedna – wzorcowa metoda stosowana w całym sektorze publicznym? Dlaczego nie wykorzystać w tym celu jednej ze znanych i sprawdzonych wcześniej metodyk?
W projekcie czytamy: „Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju – zakończenie prac planowane jest do końca 2020 roku.

Uwaga szczegółowa 7. Zwalczanie cyberprzestępczości – pkt 6 cel 2
Podkreśla się potrzebę prowadzenia badań naukowych i słusznie:
„Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych."
Niemniej znaczne efekty można także osiągnąć przez współpracę z NGO's policji i prokuratury np. współpracy Stowarzyszenia Sygnał czy BSA w zwalczaniu kradzieży własności intelektualnej poprzez organizacje wspólnych szkoleń, konferencji, opracowywanie metodyk zwalczania przestępczości określonego typu.
PIIT wystosowywała także liczne petycje w których sygnalizowała problemy związane z kradzieżą tożsamości w Internecie, podrabianiem dokumentów tożsamości zarówno polskich jak i zagranicznych, przeciwdziałaniu wyłudzeniom i oszustwom, w tym także poprzez dostęp do rejestrów i ewidencji publicznych kluczowych uczestników e-obrotu w tym operatorów telekomunikacyjnych i dostawców usług zaufania. Izba z niepokojem obserwuje narastające zjawisko wykorzystywania fałszywych dokumentów tożsamości do popełniania przestępstw na szkodę obywateli RP. Według ChronPESEL.pl tylko w 2017 roku dokonano 47 tys. wyłudzeń na skradzione dane osobowe o łącznej wartości nawet 3 mld. zł. Problem ten był wielokrotnie sygnalizowany Ministerstwu przez Izbę m.in. w związku z postępowaniami o udzielenie dostępu do Rejestru PESEL, czy Rejestru Dowodów Osobistych.
Wypunktowanie wielu zasadnych aktywności, które jednak bez wątpienia dla skutecznego przeprowadzenia wymagają niemałych środków finansowych.
Przykładowe wymienione w projekcie Strategii aktywności, które na pewno wbrew deklarowanemu, iż zapewniono są na nie środki, wymagają zarezerwowania znacznych dodatkowych środków:

- 5.4 Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym;
- 5.4 Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej;
- 7.3 Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa.

Uwaga szczegółowa 8. Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa.
Brakować zdaje się opisu działań, jakie będzie podejmowała Polska na arenie międzynarodowej w stosunku do podejrzewanych o popełnienie cyberprzestępstw, tak pojedynczych osób z innych

krajów, jak i zorganizowanych grup przestępczych oraz grup sponsorowanych przez instytucje rządowe i siły zbrojne państw prowadzących ofensywne działania w cyberprzestrzeni, ukierunkowane w szczególności na cyberszpiegostwo oraz rozpoznanie zdolności obronnych innych państw. W Strategii szeroko opisano działania na rzecz współpracy, współdziałania, wymiany informacji, reagowania na incydenty. Nie ma nic na temat dążenia Polski do skutecznego ścigania tych przestępstw, a przecież wszelkie działania ofensywne w cyberprzestrzeni są prowadzone z terytoriów innych państw. W Strategii nie znajdziemy odpowiedzi na to jak Polska poradzi sobie ze ściganiem przestępstw cyber prowadzonymi na arenie międzynarodowej, czy nawet w kraju.
Nie zostały zaadresowane ani zaznaczone wielokrotnie sygnalizowane kwestie nadużyć (tzw. fraudów) na rynku telekomunikacyjnym, polegające na wprowadzaniu klientów w błąd, podszywaniu się pod innego przedsiębiorcę, manipulowaniu podczas zawierania umowy. Obecnie w praktyce każdy przedsiębiorca telekomunikacyjny samodzielnie realizuje działania w zakresie zwalczania nadużyć telekomunikacyjnych, dzięki czemu wypracowane zostają własne metody działania, na które składają się stosowane procedury, technologie oraz zespoły pracownicze. Wdrażanie indywidualnych działań nie jest jednak wystarczające wobec braku odpowiednich rozwiązań systemowych i prawnych.
Ponadto, nadużycie telekomunikacyjne polegające na ingerencji w numer abonenta uniemożliwia identyfikację abonenta inicjującego połączenia, co ma istotne znaczenia dla realizacji obowiązków przez uprawnione podmioty (służby), ponieważ utrudnia im podejmowanie działań operacyjnych.
Brak odpowiednich regulacji prawnych oraz jednoznacznych zasad penalizacji takiej działalności może prowadzić do zagrożenia dla bezpieczeństwa państwa i ochrony porządku publicznego. Ponadto, daje możliwość dokonywania takiej podmiany przez różne organizacje przestępcze i terrorystyczne do bezpiecznej komunikacji, co w znacznym stopniu utrudnia przeciwdziałanie aktom terrorystycznym.

Uwaga szczegółowa 9. Wymagania organizacyjno - techniczne na sprzęt i oprogramowanie dla sektora publicznego
W projekcie Strategii zapisano w pkt. 6 cel 2: „W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa:
1) aplikacji,
2) urządzeń mobilnych,
3) stacji roboczych,
4) serwerów i sieci,
5) modeli chmur obliczeniowych.”
Wprowadzenie specyficznych wymagań dla sektora publicznego poprzez Narodowe Standardy Cyberbezpieczeństwa, może być wykorzystywane do wprowadzania preferencji dla określonych dostawców zaopatrujących sektor publiczny i ograniczaniu konkurencji. Obecnie państwo chętnie powierza kluczowe zadania w zakresie wytwarzania systemów informatycznych podmiotom kontrolowanym lub zarządzanym przez państwo bez przestrzegania zasad konkurencji np. w drodze stanowienia prawa. Tworzenie Narodowych Standardów Cyberbezpieczeństwa bez powiązania z międzynarodowymi może prowadzić do pogorszenia jakości specyficznie polskich rozwiązań i wymagań. Nie ma mowy o żadnej konkurencyjności rozwiązań i poprawianiu cyberbezpieczeństwa, jeżeli mają je realizować imiennie wskazywane podmioty. Budzi to poważne wątpliwości co do bezpieczeństwa przyjmowanych rozwiązań. Przypominamy także że art.67 Ustawy o Krajowym Systemie Cyberbezpieczeństwa przewiduje wydawanie, przez Prezesa Rady Ministrów, wiążących wytycznych dla sektora publicznego w zakresie Cyberbezpieczeństwa który stanowi swoisty bufor bezpieczeństwa. Istnienie tych regulacji nie uzasadnia wprowadzanie nowych opartych o bliżej niedoprecyzowane Narodowe Standardy Cyberbezpieczeństwa.

Uwaga szczegółowa 10. Polskie zasoby naukowe i kompetencyjne.
W opisie punktu „7.1 Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa" można przeczytać:
„Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-upów, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność. Pozyskiwanie nowych technologii dla rozwoju rodzimych przedsięwzięć będzie realizowane poprzez udział w inicjatywach międzynarodowych kładących nacisk na innowacyjność, w drodze współpracy dwustronnej oraz w ramach organizacji międzynarodowych, w tym w ramach planowanego przez Komisję Europejską i Państwa Członkowskie Europejskiego Centrum Kompetencji Cyberbezpieczeństwa."
O ile pozyskiwanie technologii z zagranicy jest oczywiście uzasadnione, to jednak rolą państwa powinno być przede wszystkim wymierne inwestowane w rodzime polskie nowe rozwiązania, gdyż kompetencje cyberbezpieczeństwa powinny być cechą, własnością i know how o narodowym charakterze. Państwo powinno finansować wytwarzanie rodzimych polskich rozwiązań, a nie przerzucać zagadnienie finansowania takich przedsięwzięć na środki unijne, które wymagają przeważnie programów z realizacją w zespołach wielonarodowych, niekoniecznie wskazanych w kontekście cyberbezpieczeństwa.
Wydaje się rzeczą oczywistą, że koniecznym warunkiem rozwoju i zapewnienia cyberbezpieczeństwa w Polsce jest posiadanie odpowiednich zasobów zarówno zatrudnionych w polskich podmiotach, jak i w zagranicznych oddziałach firm znajdujących się w Polsce.

Uwaga szczegółowa 11. Certyfikacja łańcucha dostaw
„Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług). Priorytetowe w tym zakresie będzie utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa, co umożliwi Polsce uzyskanie pełnego i rozpoznawanego na arenie europejskiej i międzynarodowej statusu państwa producenta w dziedzinie rozwiązań cyberbezpieczeństwa.
Polska aktywnie włączy się w prace nad ustanowieniem europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) Dz. Dz. Urz. UE L 151 z 07.06.2019.

Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego organu ds. certyfikacji cyberbezpieczeństwa, który będzie wydawał europejskie certyfikaty cyberbezpieczeństwa oraz nadzorował krajowe jednostki oceniające zgodność produktów, usług i procesów z wymaganiami określonymi w europejskich programach certyfikacji cyberbezpieczeństwa"
Wyznaczenie krajowego organu to zdecydowanie za mało by projekt się udał. Istnieje przede wszystkim potrzeba zapewnienia mu odpowiednich środków finansowych i narzędzi do prowadzenia badań.

Uwaga szczegółowa 12. Niedostateczne uwzględnienie współpracy publiczno-prywatnej w zakresie cyberbezpieczeństwa (Rozdział 7, strona 17 i następne)

Uważamy, że temat został potraktowany zbyt ogólnikowo. Administracja, nie tylko polska, wykorzystuje na wielką skalę produkty i usługi przygotowane przez podmioty komercyjne. Producenci i usługodawcy wydają na zagadnienia związane z cyberbezpieczeństwem kwoty porównywalne z nakładami ponoszonymi przez poszczególne państwa. Mają także wyspecjalizowane usługi i zespoły dedykowane do zagadnień cyberbezpieczeństwa. Współpraca z producentami i usługodawcami jest praktycznym zapewnieniem wyższego poziomu cyberbezpieczeństwa w najkrótszym czasie.
Uważamy, że programy oceny i certyfikacji (jak opisane w pkt. 6.2. Strategii) stanowią wyłącznie wymaganie formalne, natomiast warunkiem rzeczywistego podniesienia cyberbezpieczeństwa będzie stworzenie faktycznych ram współpracy. Naszym zdaniem z punktu widzenia Strategii należałoby określić przynajmniej (Propozycja poniżej):

1) Listę producentów i dostawców usług cyfrowych o kluczowym znaczeniu dla cyberbezpieczeństwa RP w latach 2019-2024. Obecność na liście musi wynikać z powszechności stosowania określonych rozwiązań i/lub z funkcji istotności takich rozwiązań dla działania państwa.
2) Określenie strategicznych celów współpracy z tymi dostawcami. W szczególności powinno to dotyczyć sposobów wymiany informacji istotnej dla cyberbezpieczeństwa, podniesienia wiedzy i umiejętności związanej z cyberbezpieczeństwem rozwiązań tych dostawców w administracji (por. cel szczegółowy 8.1.) oraz innych aspektów współpracy.
3) Wskazanie i zapewnienie odpowiednich zasobów oraz właściwego centrum współpracy dla wszystkich wybranych producentów i dostawców.
4) Określenie zasad współpracy międzynarodowej w ramach współdziałania z tymi samymi producentami i dostawcami w wielu krajach UE.
5) Określenia zasad współpracy w/w dostawców z polskimi podmiotami istotnymi dla cyberbezpieczeństwa państwa (np. operatorami usług kluczowych) wdrażającymi technologie tych dostawców. Przykładem mogą być minimalne warunki suportu technicznego jakie odbiorca musi mieć zapewnione przy wdrożeniu, przy jednoczesnym zachowaniu zasady neutralności technologicznej zapisanej w ustawie o informatyzacji, tzn. brak dyskryminacji takiego podmiotu komercyjnego wynikający z faktu, że inne rozwiązanie, gdzie suport nie jest wymagany staje się automatycznie tańsze i bardziej atrakcyjne.

Naszym zdaniem, aby w szybki sposób podnieść poziom cyberbezpieczeństwa wymagane byłoby wskazanie podmiotów komercyjnych, z którymi prowadzona byłaby sformalizowana i programatyczna współpraca w ramach cyberbezpieczeństwa. Listę tę można poddawać każdego roku odpowiedniej weryfikacji.

Uwaga szczegółowa 13. Mechanizmy współpracy z sektorem prywatnym
W pkt. zatytułowanym „zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym” zawarta jest sugestia, że takie mechanizmy dopiero musza być budowane tzn., że ich jakoby nie ma.
Po pierwsze: pewne mechanizmy istnieją np. konsultacji projektów przepisów, spotkań tematycznych, udziału w konferencjach obu sektorów, etc. Rada ds. cyfryzacji także w pewnym stopniu służy tym celom choć naszym zdaniem z niedostateczna reprezentacja sektora prywatnego/biznesowego. Dobrym przykładem na współprace sektorów jest praca grup roboczych nad wdrożeniem ustawy o krajowym systemie cyberbezpieczeństwa i wypracowywane w jej ramach opinie i opracowania.
„Jednocześnie administracja publiczna będzie doskonaliła swój potencjał w zakresie inicjowania i prowadzenia projektów w dziedzinie cyberbezpieczeństwa. Rząd będzie również aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej i tym samym będzie promować polski biznes na arenie międzynarodowej”.

Chcielibyśmy zapytać także o jakich powstających formach europejskiej współpracy publiczno-prywatnej jest mowa w tym pkt?

Uwaga szczegółowa 14. Zarządzanie Strategią - niespójność
W pkt. 10 mówi się o przeglądzie Strategii co dwa lata:
Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. Wyniki przeglądu przedstawiane są Radzie Ministrów."
Zaś sam projekt uchwały Rady ministrów w par. 3 zobowiązuje Ministra właściwego do corocznego przedstawiania sprawozdania.

Opinia Polskiej Izby Informatyki i Telekomunikacji (PIIT)
w sprawie Rekomendacji Komisji Europejskiej dot. Cyberbezpieczeństwa w sieci 5G Strasbourg, 26.3.2019 C(2019) 2335 final

Jesteśmy gorącymi zwolennikami rozwoju sieci 5G widząc w nich narzędzie do zwielokrotnienia kilkadziesiąt razy przepustowości sieci i konieczny warunek dalszego rozwoju tzw. Przemysłu 4.0, a w szerszym aspekcie - demokratycznego społeczeństwa opartego o nowoczesne technologie.
W związku z przygotowywaną przez Rząd RP, jako kraj członkowski Unii Europejskiej, analizą ryzyk, zgodnie z procedurami przyjętymi przez Komisję Europejską pragniemy zwrócić uwagę Polskiego Rządu na najistotniejsze zagrożenia związane z cyberbezpieczeństwem w budowie sieci 5G w Polsce.

I. Zagrożenia natury ogólnej

1. Opowiadamy się za zgodną współpracą z wszystkimi krajami na świecie - w tym z ChRL, ponieważ pracujemy dla firm ICT i nie zajmujemy się polityką. Jako Polacy wspieramy jednak przynależność RP do wspólnoty transatlantyckiej - NATO - jako gwaranta naszego bezpieczeństwa i ducha tego przymierza. Nie możemy bowiem pozostawać obojętni na liczne sygnały dot. zagrożeń związanych z budowa sieci 5G zwłaszcza przez dostawców dalekowschodnich.

Komisja Europejska w rekomendacjach zwraca uwagę, że oprócz zagrożeń technologicznych państwa członkowskie powinny zwrócić uwagę także na inne zagrożenia (pkt. 20 rekomendacji).

II. Ryzyka związane wytwarzaniem oprogramowania

Nasze zaniepokojenie budzą następujące ryzyka sygnalizowane przez poważne instytucje publiczne związane z potencjalnym udziałem chińskich firm w budowie sieci 5G:
1.Ryzyka związane z niskim poziomem wytwarzania oprogramowania.
2. W naszej ocenie, ani Polska ani UE nie dysponuje obecnie potencjałem organizacyjnym czy eksperckim, który pozwoliłby w sposób ciągły i przewidywalny badać oprogramowanie nawet z pełnym kodem źródłowym w skali systemów operacyjnych dostarczane przez strony trzecie.
3. Co więcej, oprogramowanie w sieciach telekomunikacyjnych jest złożone z dużej ilości (dziesiątek, czasami setek) modułów, które są często aktualizowane. Certyfikacja jednej konkretnej jego wersji jest nie tylko czasochłonna, ale również ograniczona tylko do tej konkretnej, certyfikowanej wersji. Z uwagi na fakt, że w sieciach operatorskich wydzielona sieć przeznaczona do zarządzania umożliwia zwykle dostęp autoryzowanym użytkownikom zdalnie, kolejnym ryzykiem mogłoby być dogrywanie już po okresie certyfikacji dodatkowych modułów.
Samo odłączenie możliwości zarządzania zdalnego również nie rozwiązuje problemu, ponieważ jest niemożliwością nawet dla wysokiej klasy specjalisty bezpieczeństwa czy też inżyniera sieciowego zbadania poprawki systemowej w wersji binarnej, lub porównanie kodu źródłowego z jego binarną wersją.
Oznacza to, że z uwagi na historycznie doświadczenia, procesy certyfikacyjne urządzeń i oprogramowania przestają mieć znaczenie jako gwarancja bezpieczeństwa.

III. Niektóre ryzyka technologiczne związane z wdrażaniem prawie każdej nowej technologii

Każda nowa technologia rodzi pewne ryzyka. Technologia 5G pozostaje w ścisłym związku z rozwojem sieci i współczesnych systemów IT, co przejawia się w nowych zagrożeniach, koniecznych do uwzględnienia - na przykład:

1. W związku z rozwojem internetu rzeczy - IoT & M2M - praktycznie brak wbudowanych mechanizmów bezpieczeństwa i autocertyfikacji rozwiązań IoT. Obecna tendencja w badaniu

tych systemów pozwala założyć, że nie da się efektywnie zabezpieczyć każdego z nich, a zatem jeszcze większy nacisk kładziony jest na bezpieczeństwo infrastruktury tak, aby zapewniała segmentację tych rozwiązań od siebie. Wzrasta zagrożenie atakami horyzontalnymi pomiędzy takimi urządzeniami.

2. Wraz z wszechobecną wirtualizacją, kolejnym poważnym wyzwaniem bezpieczeństwa staje się konwergencja wielu technologii - bez stabilnej, bezpiecznej platformy, wydaje się niemożliwe zabezpieczenie całości rozwiązania (czyli np. sieci 5G).
3. Wymóg na minimalne opóźnienia sygnału (w sieciach 5G) uniemożliwia w praktyce wbudowanie silnych mechanizmów ochronnych jak w tradycyjnych sieciach a może powodować fałszywe poczucie bezpieczeństwa przez szyfrowanie w warstwie użytkownika - bez możliwości inspekcji przez operatora, lub uprawnione służby czy transmisja faktycznie zawiera tylko i wyłącznie dane nadawane i odbierane przez uprawnionych członków dyskusji/transmisji.

Te rodzaje zagrożeń może być jednak skutecznie niwelowane w ramach współpracy pomiędzy państwami wewnątrz UE w oparciu o Cybersecurity Act, procesy certyfikacji i współpracę z ENISA.

Te ryzyka minimalizuje też zaufanie do sprawdzonych dostawców technologii w tym zrzeszonych w PIIT.

Wnioski

W związku z powyższymi ryzykami powinny zostać przyjęte przez rząd i parlament adekwatne do nich środki zabezpieczające, zgodnie z postulatem Komisji Europejskiej: http://europa.eu/rapid/press-release_IP-19-1832_pl.htm w którym czytamy m.in., że:

„Każde państwo członkowskie powinno do końca czerwca 2019 r. przeprowadzić krajową ocenę ryzyka związanego z infrastrukturą sieci 5G. Na tej podstawie państwa członkowskie powinny zaktualizować dotychczasowe wymogi w zakresie bezpieczeństwa, którym podlegają dostawcy usług sieciowych, oraz wprowadzić warunki gwarantujące bezpieczeństwo sieci publicznych, zwłaszcza przy przyznawaniu praw użytkowania częstotliwości radiowych w pasmach 5G. Środki te powinny obejmować nałożenie na dostawców i operatorów zaostrzonych wymogów, zobowiązujących ich do zapewnienia bezpieczeństwa sieci. Krajowe oceny ryzyka oraz środki powinny uwzględniać różne czynniki ryzyka, takie jak ryzyko techniczne oraz ryzyko związane z zachowaniem dostawców lub operatorów, w tym dostawców i operatorów z państw trzecich. Krajowe oceny ryzyka będą stanowić centralny element w procesie opracowywania skoordynowanej unijnej oceny ryzyka.
Państwa członkowskie UE mają prawo wykluczyć przedsiębiorstwa ze swoich rynków ze względów bezpieczeństwa narodowego, jeżeli przedsiębiorstwa te nie przestrzegają norm i przepisów obowiązujących w danym państwie.”

Zdanie odrębne:

Huawei Polska sp. z o.o. zgłasza zdanie odrębne do przedmiotowej opinii wskazując, że:

1. zidentyfikowane w niej ryzyka, można odnieść w całej rozciągłości do wszelkich dostawców bez względu na kraj pochodzenia;
2. dokument niniejszy naszym zdaniem nie stanowi istotnego wkładu w dyskusję o cyberbezpieczeństwie sieci 5G.