Nieformalne spotkanie ministrów telekomunikacji
w dniach 4-5 marca 2025 r. w Warszawie
Apel Warszawski w sprawie wyzwań związanych z cyberbezpieczeństwem

Szybki postęp w dziedzinie technologii cyfrowych, pojawienie się nowych zagrożeń cybernetycznych i zmiany w sytuacji geopolitycznej doprowadziły UE i jej państwa członkowskie do punktu zwrotnego. Ponieważ dążymy do utrzymania silnej i bezpiecznej gospodarki, potrzeba wzmocnienia cyberbezpieczeństwa we wszystkich sektorach nigdy nie była tak pilna.

Trwająca agresja Rosji przeciwko Ukrainie stworzyła nowy kontekst strategiczny i potwierdziła potrzebę dalszego wzmacniania przez UE, jej państwa członkowskie i ich partnerów odporności na zagrożenia cybernetyczne oraz zwiększenia naszego wspólnego bezpieczeństwa cybernetycznego i cyberobrony przed złośliwymi działaniami i aktami agresji w cyberprzestrzeni.

Świadomi, że gotowość i współpraca są niezbędne dla zachowania cyberbezpieczeństwa, my, ministrowie odpowiedzialni za cyberbezpieczeństwo, jednogłośnie:

1. **Wzywamy do terminowego przyjęcia unijnego planu zarządzania kryzysowego w zakresie cyberbezpieczeństwa (Cyber Blueprint),** który jest niezbędnym narzędziem do sprostania obecnym wyzwaniom i złożonemu środowisku zagrożeń cybernetycznych, wzmocnienia istniejących sieci, zacieśnienia współpracy i przełamania barier między organizacjami, wykorzystując w tym celu przede wszystkim istniejące struktury. Podkreślamy **potrzebę przetestowania Cyber Blueprint w ramach ćwiczeń** po jego przyjęciu.
2. Podkreślamy potrzebę dalszego **zacieśniania współpracy i wymiany informacji na temat cyberbezpieczeństwa między** państwami członkowskimi a podmiotami UE za pośrednictwem istniejących struktur.
3. Przypominamy o **potrzebie zacieśnienia współpracy cywilno-wojskowej** w dziedzinie cyberbezpieczeństwa, w szczególności w obszarach strategicznych, takich jak świadomość sytuacyjna i zarządzanie kryzysowe, w tym współpracy UE-NATO, przy pełnym

poszanowaniu zasad inkluzywności, wzajemności i autonomii decyzyjnej obu organizacji.

4. Wzywamy do kontynuacji i dalszego rozwoju **ocen ryzyka cyberbezpieczeństwa**, w tym scenariuszy ryzyka na poziomie UE dla wszystkich kluczowych sektorów, zainicjowanych przez apel w Nevers i konkluzje Rady w sprawie rozwoju postawy Unii Europejskiej w obszarze cyberbezpieczeństwa.

5. Podkreślamy potrzebę trwałego i strategicznego **wykorzystania pełnego spektrum środków w ramach zestawu narzędzi dla dyplomacji cyberbezpieczeństwa** oraz wzmocnienia powiązań z zestawami narzędzi hybrydowych i FIMI, w stosownych przypadkach, w celu zapobiegania, odstraszania i reagowania na złośliwe działania w cyberprzestrzeni ze strony podmiotów państwowych i niepaństwowych.

6. Ponownie podkreślamy, że **dyrektywa NIS 2 powinna być głównym horyzontalnym aktem prawnym dotyczącym cyberbezpieczeństwa** i zdecydowanie przestrzegamy przed fragmentacją, powielaniem lub nakładaniem się przepisów dotyczących cyberbezpieczeństwa w całej UE w ramach inicjatyw sektorowych lub lex specialis.

7. Podkreślamy potrzebę skupienia się na **zharmonizowanym i sprzyjającym innowacjom wdrażaniu przepisów dotyczących cyberbezpieczeństwa oraz znalezienia sposobów na uproszczenie** i zmniejszenie obciążeń, jak na przykład ustanowienie pojedynczych punktów przyjmowania zgłoszeń.

8. Podkreślamy potrzebę zaangażowania się w regularny dialog i wzmocnienia **unijnej ekspertyzy co do prognozowania strategicznego w obszarze cyberbezpieczeństwa** w celu lepszego przewidywania i przygotowania się na przyszłe cyber zagrożenia.

9. Podkreślamy potrzebę opracowania **skoordynowanego planu wdrożenia nowych technologii mających wpływ na cyberbezpieczeństwo**, który uwzględniałby zarówno możliwości, jak i zagrożenia, biorąc pod uwagę skoordynowany plan wdrożenia przejścia na kryptografię postkwantową.

10. Podkreślamy znaczenie dalszej harmonizacji działań na rzecz **inwestycji w cyberbezpieczeństwo** oraz wspierania misji Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) w celu stworzenia silnego

i konkurencyjnego europejskiego ekosystemu przedsiębiorstw zajmujących się cyberbezpieczeństwem. Podkreślamy korzyści płynące z tworzenia synergii między **inwestycjami obronnymi i cywilnymi** oraz między sektorami badań, inwestycji i biznesu w dziedzinie cyberbezpieczeństwa.

11. Wzywamy do zwiększenia wysiłków **na rzecz zwalczania niedoboru specjalistów ds. cyberbezpieczeństwa w UE,** na przykład w ramach Akademii Umiejętności w zakresie Cyberbezpieczeństwa, w tym poprzez promowanie wdrażania europejskich ram umiejętności w zakresie cyberbezpieczeństwa opracowanych przez Agencję UE ds. Cyberbezpieczeństwa (ENISA) oraz poprzez zaangażowanie państw członkowskich za pośrednictwem ECCC i sieci NCC.

12. Uznajemy **kluczową rolę wspierającą** ENISA w podnoszeniu poziomu cyberbezpieczeństwa w UE i państwach członkowskich oraz potrzebę wzmocnienia, jasnego zdefiniowania i ukierunkowania przyszłego mandatu ENISA**.**

13. Zachęcamy do podejmowania zwiększonych i bardziej skoordynowanych wysiłków w celu **egzekwowania ochrony infrastruktury kabli podmorskich** przed zagrożeniami, zarówno fizycznymi, jak i cyber, z należytym poszanowaniem wyłącznych kompetencji państw członkowskich w zakresie bezpieczeństwa narodowego. Przyjmujemy do wiadomości Plan działania na rzecz lepszego zabezpieczenia kabli podmorskich przedstawiony przez Komisję i Wysokiego Przedstawiciela oraz oczekujemy jego wdrożenia w całej Unii Europejskiej w świetle ostatnich incydentów, zwłaszcza na Morzu Bałtyckim.

Niniejszy Apel Warszawski podkreśla nasze zaangażowanie w budowanie bezpieczniejszej i bardziej odpornej gospodarki oraz ochronę naszego europejskiego stylu życia. Pozostajemy skoncentrowani na zapewnieniu, że transformacja cyfrowa opiera się na solidnych fundamentach cyberbezpieczeństwa, zakorzenionych w prawie międzynarodowym i prawach człowieka w całej Unii Europejskiej.

Wzywamy Unię Europejską i jej państwa członkowskie do utrzymania zaangażowania w umacnianie cyberbezpieczeństwa we wszystkich sektorach, aby zapewnić odporność unijnej infrastruktury cyfrowej w obliczu dynamicznie ewoluujących zagrożeń i nowych wyzwań w zakresie bezpieczeństwa.