



Rada  
Unii Europejskiej

**Bruksela, 19 czerwca 2017 r.  
(OR. en)**

**10474/17**

**CYBER 98  
RELEX 554  
POLMIL 77  
CFSP/PESC 557**

**WYNIK PRAC**

---

Od:	Sekretariat Generalny Rady
Data:	19 czerwca 2017 r.
Do:	Delegacje

---

Nr poprz. dok.:	9916/17
-----------------	---------

---

Dotyczy:	Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”), 19 czerwca 2017 r.
----------	---

---

Delegacje otrzymują w załączeniu konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”) przyjęte przez Radę do Spraw Zagranicznych na jej 3551. posiedzeniu 19 czerwca 2017 r.

**KONKLUZJE RADY W SPRAWIE RAM WSPÓLNEJ UNIJNEJ REAKCJI  
DYPLOMATYCZNEJ NA SZKODLIWE DZIAŁANIA CYBERNETYCZNE („ZESTAW  
NARZĘDZI DLA DYPLOMACJI CYFROWEJ”)**

**Rada Unii Europejskiej przyjęła następujące konkluzje:**

1. UE uznaje, że cyberprzestrzeń oferuje znaczne możliwości, ale stawia także stale zmieniające się wyzwania przed politykami zewnętrznymi UE, w tym przed wspólną polityką zagraniczną i bezpieczeństwa; UE podkreśla też rosnącą potrzebę chronienia integralności i bezpieczeństwa UE, jej państw członkowskich oraz ich obywateli przed zagrożeniami cybernetycznymi i szkodliwymi działaniami cybernetycznymi.

UE przypomina swoje konkluzje w sprawie strategii bezpieczeństwa cybernetycznego UE<sup>1</sup>, w szczególności swoją determinację, by cyberprzestrzeń pozostała otwarta, wolna, stabilna i bezpieczna oraz by w pełni stosowano w niej prawa podstawowe i praworządność. Przywołuje także swoje konkluzje w sprawie dyplomacji elektronicznej<sup>2</sup>, w szczególności stwierdzenie, że wspólne i całościowe unijne podejście do dyplomacji cyfrowej mogłoby przyczynić się do zapobiegania konfliktom, zmniejszenia zagrożeń dla bezpieczeństwa cybernetycznego oraz do wzrostu stabilności w stosunkach międzynarodowych.

UE i jej państwa członkowskie zwracają uwagę na znaczenie stałego zaangażowania UE w dziedzinie dyplomacji cyfrowej oraz na potrzebę spójności między inicjatywami UE w odniesieniu do cyberprzestrzeni w celu skutecznego wzmocnienia odporności cybernetycznej, i są zachęcane do dalszego zwiększania wysiłków na rzecz dialogu w sprawie cyberprzestrzeni w ramach skutecznej koordynacji polityki, oraz podkreślają, jak ważne jest budowanie zdolności cyfrowych w państwach trzecich.

2. UE jest zaniepokojona rosnącą zdolnością i gotowością podmiotów państwowych i niepaństwowych do realizowania swoich celów za pomocą szkodliwych działań cybernetycznych o różnym zakresie, skali, czasie trwania, intensywności, złożoności, zaawansowaniu i skutkach.

---

<sup>1</sup> Dok. 12109/13.

<sup>2</sup> Dok. 6122/15.

UE potwierdza, że szkodliwe działania cybernetyczne mogą w świetle prawa międzynarodowego stanowić akty bezprawne, i podkreśla, że żadne państwo nie powinno prowadzić ani świadomie wspierać działań w zakresie ICT naruszających ich obowiązki wynikające z prawa międzynarodowego, oraz że nie powinno świadomie dopuszczać do wykorzystywania swojego terytorium do bezprawnych w świetle prawa międzynarodowego działań z wykorzystaniem ICT, jak stwierdzono w sprawozdaniu grupy ekspertów rządowych ONZ z 2015 r.

3. UE przypomina o czynionych przez nią i jej państwa członkowskie wysiłkach na rzecz poprawy odporności cybernetycznej, w szczególności poprzez wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz ustanowienie mechanizmów współpracy operacyjnej w niej przewidzianych, oraz przypomina że szkodliwe działania cybernetyczne względem systemów informacyjnych, zgodnie z definicją zawartą w prawie UE, stanowią przestępstwo, i że skuteczne dochodzenie i ściganie takich przestępstw pozostaje wspólnym przedsięwzięciem państw członkowskich.

UE i jej państwa członkowskie odnotowują trwające prace oenztowskiej grupy ekspertów rządowych ds. sytuacji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego, opierające się na sprawozdaniach z lat 2010, 2013 i 2015<sup>3</sup>, i są zachęcane do zdecydowanego popierania osiągniętego konsensusu, zgodnie z którym do cyberprzestrzeni ma zastosowanie prawo międzynarodowe. UE i jej państwa członkowskie zdecydowanie zobowiązują się do aktywnego wspierania opracowywania dobrowolnych niewiążących norm odpowiedzialnego zachowania państw w cyberprzestrzeni i uzgodnionych przez OBWE środków budowy zaufania w regionie<sup>4</sup>, aby zmniejszyć ryzyko konfliktów wynikających z korzystania z technologii informacyjnych i komunikacyjnych.

UE potwierdza swoje zaangażowanie na rzecz rozstrzygania międzynarodowych sporów w cyberprzestrzeni środkami pokojowymi, oraz potwierdza, że wszystkie działania dyplomatyczne UE powinny być w pierwszej kolejności nakierowane na propagowanie bezpieczeństwa i stabilności w cyberprzestrzeni poprzez zacieśnienie współpracy międzynarodowej oraz na zmniejszanie ryzyka nieporozumień, eskalacji i konfliktu, które mogą wynikać z incydentów w dziedzinie ICT. W tym względzie UE przypomina apel Zgromadzenia Ogólnego ONZ skierowany do państw członkowskich ONZ, by przy korzystaniu z technologii ICT kierowały się zaleceniami zawartymi w sprawozdaniach oenztowskiej grupy ekspertów rządowych.

---

<sup>3</sup> A/68/98 i A/70/174.

<sup>4</sup> PC.DEC/1106 z dnia 3 grudnia 2013 r. i PC.DEC/1202 z dnia 10 marca 2016 r.

4. UE podkreśla, że wyraźne sygnalizowanie prawdopodobnych konsekwencji, jakie nastąpią w wyniku wspólnej unijnej reakcji dyplomatycznej na takie szkodliwe działania cybernetyczne, wpływa na zachowania potencjalnych agresorów w cyberprzestrzeni i tym samym wzmacnia bezpieczeństwo UE i jej państw członkowskich. UE przypomina, że kwestia ustalenia, który podmiot państwowy lub niepaństwowy ponoszą odpowiedzialność za takie działania, w dalszym ciągu podlega suwerennej decyzji politycznej opartej na danych wywiadowczych pochodzących z wszelkich źródeł; powinno to przebiegać zgodnie z międzynarodowym prawem dotyczącym odpowiedzialności państw. UE podkreśla w tym względzie, że nie wszystkie środki wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne wymagają ustalenia odpowiedzialnego podmiotu państwowego lub niepaństwowego.

5. UE potwierdza, że środki przewidziane w ramach wspólnej polityki zagranicznej i bezpieczeństwa, w tym w razie konieczności środki ograniczające, przyjmowane zgodnie z odpowiednimi postanowieniami traktatów stanowią odpowiednie ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne i powinny zachęcać do współpracy, ułatwiać ograniczanie bezpośrednich i długoterminowych zagrożeń oraz w perspektywie długoterminowej wpływać na zachowania potencjalnych agresorów. UE będzie pracować nad dalszym rozwijaniem ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne, kierując się następującymi głównymi zasadami. Ramy te powinny:

- służyć ochronie integralności i bezpieczeństwa UE, jej państw członkowskich i ich obywateli,
- uwzględniać szerszy kontekst stosunków zewnętrznych utrzymywanych przez UE z danym państwem,
- przewidywać osiągnięcie celów WPZiB określonych w Traktacie o Unii Europejskiej (TUE) i stosowanie odnośnych procedur przewidzianych dla osiągnięcia tych celów,
- być oparte na uzgodnionej przez państwa członkowskie orientacji sytuacyjnej i odpowiadać potrzebom konkretnych sytuacji,
- być proporcjonalne do zakresu, skali, czasu trwania, intensywności, złożoności, zaawansowania i skutków działania cybernetycznego,
- być zgodne z mającym zastosowanie prawem międzynarodowym i nie mogą naruszać podstawowych praw i wolności.

6. UE wzywa państwa członkowskie, Europejską Służbę Działań Zewnętrznych (ESDZ) i Komisję, by w pełni zrealizowały zadanie polegające na opracowaniu ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne i w tym względzie potwierdza swoje zaangażowanie na rzecz kontynuowania prac w zakresie tych ram we współpracy z Komisją, ESDZ i innymi odnośnymi stronami poprzez ustanawianie wytycznych dotyczących wdrażania, w tym opracowywanie praktyk przygotowawczych i procedur komunikacji oraz ich testowanie za pomocą odpowiednich ćwiczeń.