Rada
Unii Europejskiej

Bruksela, 7 czerwca 2017 r.
(OR. en)

9916/17

CYBER 91
RELEX 482
POLMIL 58
CFSP/PESC 476

NOTA DO PUNKTU I/A

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli / Rada
Nr poprz. dok.:	7923/2/17 REV 2
Dotyczy:	Projekt konkluzji Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”) – Przyjęcie

1. Na posiedzeniu Komitetu Politycznego i Bezpieczeństwa (KPiB) w dniu 14 marca 2017 r. ESDZ i służby Komisji przedstawiły wspólny dokument tematyczny dotyczący wspólnej unijnej reakcji dyplomatycznej na operacje cybernetyczne („zestaw narzędzi dotyczących cyberprzestrzeni”)[1]. Dokument ten został przyjęty przez delegacje z zadowoleniem, podobnie jak zaproponowane działania następcze do niego w ramach horyzontalnej grupy roboczej ds. cyberprzestrzeni (HWPCI). W rezultacie KPiB zwrócił się do HWPCI, aby bardziej szczegółowo przeanalizowała ten dokument tematyczny, w stosownych przypadkach w porozumieniu z innymi organami przygotowawczymi Rady, zanim KPiB powróci do tej kwestii przed końcem czerwca z uwzględnieniem wyniku tych analiz.

2. W związku z powyższą prośbą KPiB wspólny dokument tematyczny został także przedstawiony i omówiony na posiedzeniu HWPCI w dniu 22 marca 2017 r. Delegacje z zadowoleniem przyjęły dokument, podkreślając jednakże, że szczegółowe omówienie tej kwestii wymagać będzie czasu. W ramach kolejnego kroku wiele z nich opowiedziało się za tym, by opracować konkluzje Rady, które towarzyszyłyby temu zestawowi narzędzi.

[1] WK 2569/2017 INIT.

3. W związku z tym prezydencja przygotowała projekt konkluzji Rady, który zawarto w dok. 7923/17 i który został przedstawiony i omówiony na dwóch kolejnych posiedzeniach HWPCI, odpowiednio w dniu 19 kwietnia i 12 maja 2017 r.; w wyniku tych posiedzeń tekst został dodatkowo uproszczony i udoskonalony zgodnie z uwagami przekazanymi przez państwa członkowskie.

4. W dniu 6 czerwca 2017 r. ostateczny tekst projektu konkluzji Rady został przedstawiony KPiB zgodnie z marcowymi ustaleniami i – z myślą o przyjęciu tych konkluzji przez Radę – uzgodniono kilka uzupełnień[2].

5. W związku z powyższym Coreper jest proszony o zwrócenie się do Rady, by zatwierdziła projekt konkluzji Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne, w wersji przedstawionej w załączniku.

---

[2] WK 6162/2017 REV 1.

ZAŁĄCZNIK

PROJEKT KONKLUZJI 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[3], 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[4], w szczególności stwierdzenie, że wspólne i całościowe unijne podejście do dyplomacji elektronicznej może 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 rozmaitym zakresie, skali, czasie trwania, intensywności, złożoności, zaawansowaniu i skutkach.

---

[3] 12109/13.
[4] 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 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 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 oenzetowskiej grupy ekspertów rządowych ds. sytuacji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego, opierające się na sprawozdaniach z lat 2010, 2013 i 2015[5], 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[6], 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 oenzetowskiej grupy ekspertów rządowych.

---

5 A/68/98 i A/70/174.

6 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 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, jaki 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 łagodzenie 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 osiąganie 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.