Wersja robocza tłumaczenia

**Oświadczenie grupy roboczej**
Grupa robocza Procesu Warszawskiego ds. cyberbezpieczeństwa
Seul, Republika Korei
7-8 października 2019 roku

Grupa robocza Procesu Warszawskiego ds. cyberbezpieczeństwa spotkała się w Seulu, w Republice Korei, 7-8 października 2019 roku. Posiedzeniu przewodniczyły wspólnie Republika Korei, Polska i Stany Zjednoczone.

Szybki rozwój Internetu i technologii informacyjno-telekomunikacyjnych nie tylko spowodował dalekosiężne zmiany w globalnej gospodarce, ale również ujawnił nowe, nieznane wcześniej zagrożenia dla międzynarodowego pokoju i bezpieczeństwa. Obserwujemy wzrost liczby destabilizujących działań w cyberprzestrzeni na całym świecie, również na Bliskim Wschodzie. Wynika to z faktu, iż państwa i podmioty niepaństwowe, dzięki rosnącej dostępności złośliwego oprogramowania, które może być użyte zarówno do celów przestępczych, jak i komercyjnych oraz powszechności urządzeń z dostępem do Internetu, mają coraz więcej możliwości prowadzenia szkodliwych i niebezpiecznych działań w cyberprzestrzeni.

Współpraca między państwami jest dziś ważniejsza niż kiedykolwiek wcześniej. Zwiększa ona stabilność i pomaga zapobiegać konfliktom, które mogą być wywołane przez szkodliwe działania w cyberprzestrzeni. Biorąc pod uwagę fakt, że różne państwa posiadają zróżnicowane, wyjątkowe kompetencje w tym zakresie, aby zwiększyć cyberbezpieczeństwo na poziomie krajowym i regionalnym, niezbędna jest pogłębiona współpraca i partnerstwo w wymiarze międzynarodowym. Grupa robocza ds. cyberbezpieczeństwa daje możliwość zacieśnienia współpracy dot. krytycznych aspektów cyberbezpieczeństwa z regionalnymi partnerami poprzez wykorzystanie wiedzy i doświadczeń, jakimi dysponują kraje całego świata.

Grupa robocza zastosowała dwutorowe podejście, uwzględniając działania ONZ w tym zakresie. W pierwszej kolejności skoncentrowała się na praktycznych działaniach, jakie państwa w regionie mogą podjąć, aby rozwijać i wzmacniać regionalny potencjał cyberbezpieczeństwa. Następnie, na działaniach politycznych promujących mechanizmy współpracy służące zapobieganiu poważnym incydentów w cyberprzestrzeni i reagowaniu na nie.

W odniesieniu do mechanizmów współpracy w zakresie reagowania na poważne incydenty cybernetyczne, delegacje omówiły: kluczowe znaczenie wymiany najlepszych praktyk z zakresu cyberbezpieczeństwa; budowanie potencjału reagowania na incydenty cybernetyczne; walkę z cyberprzestępczością przy uwzględnieniu budapeszteńskiej Konwencji Rady Europy o cyberprzestępczości; oraz rozwój i wdrażanie narodowych strategii cybernetycznych. Grupa robocza będzie pracować nad praktycznymi aspektami, w tym procedurami i narzędziami umożliwiającymi skuteczniejsze rozpoznanie zagrożenia cybernetycznego i wymianę informacji, jak również szybsze gromadzenie i wymianę znalezionych w Internecie dowodów. Celem tych prac będzie zwiększenie możliwości rozpoznania i odpowiedzi na cyberzagrożenia, zgodnie z ustaleniami podjętymi na forum ONZ.

W odniesieniu do inicjatyw promujących współpracę w zapobieganiu i reagowaniu na poważne incydenty cybernetyczne, delegacje omówiły, w jaki sposób ramowe założenia gwarantujące stabilność w cyberprzestrzeni, wypracowane przez Grupę Ekspertów Rządowych ONZ i rekomendowane przez Zgromadzenie Ogólne ONZ, mogą przyczynić się do zwiększenia bezpieczeństwa we wszystkich regionach. Wspomniane ramowe założenia zawierają trzy zasadnicze elementy: 1) potwierdzenie, że istniejące prawo międzynarodowe ma zastosowanie do podejmowanych przez państwa działań w cyberprzestrzeni; 2) przyjęcie dobrowolnych, niewiążących norm dot. odpowiedzialnych działań podejmowanych przez państwa w cyberprzestrzeni w czasie pokoju; i 3) rozważenie, rozwój i wdrażanie praktycznych środków budowy zaufania (CBM) w celu zmniejszenia ryzyka konfliktu w cyberprzestrzeni.

Państwa członkowskie ONZ zobowiązały się już do przestrzegania tych ramowych założeń w swoich działaniach, a grupa robocza omówiła zwiększenie wsparcia dla tych założeń w celu poprawy stabilności regionalnej i bezpieczeństwa. Członkowie grupy roboczej rozmawiali również o dodatkowych inicjatywach, zmierzających do powstrzymania podmiotów przed prowadzeniem destabilizujących działań w cyberprzestrzeni oraz mających na celu pociągnięcie do odpowiedzialności podmiotów podejmujących szkodliwe działania. Grupa omówiła też zwiększenie wsparcia dla wzmacniania zdolności oraz innych środków budowy zaufania, w tym tworzenia punktów kontaktowych i wymiany informacji o narodowych cyberstrategiach lub programach, co jest kolejnym kluczowym sposobem wspierania wspomnianych założeń ramowych i szerszej regionalnej stabilności. Grupa uznała znaczenie międzyregionalnej współpracy dla skutecznego reagowania na zagrożenia cybernetyczne. Mogłaby ona obejmować m. in. wymianę informacji w zakresie najlepszych praktyk regionalnych dotyczących środków budowy zaufania i inicjatyw w zakresie budowania zdolności.

Poniższe kraje brały udział w formułowaniu oświadczenia grupy roboczej:

1. Afganistan
2. Arabia Saudyjska
3. Australia
4. Austria
5. Bahrajn
6. Belgia
7. Brazylia
8. Chorwacja
9. Czarnogóra
10. Dania
11. Ekwador
12. Egipt
13. Estonia
14. Finlandia
15. Francja

16. Grecja
17. Hiszpania
18. Holandia
19. Irlandia
20. Izrael
21. Jordania
22. Katar
23. Kolumbia
24. Kuwejt
25. Łotwa
26. Maroko
27. Meksyk
28. Niemcy
29. Nowa Zelandia
30. Nigeria
31. Norwegia
32. Oman
33. Polska
34. Portugalia
35. Czechy
36. Republika Korei
37. Rumunia
38. Słowacja
39. Stany Zjednoczone
40. Szwajcaria
41. Tunezja
42. Ukraina
43. Wielka Brytania
44. Węgry
45. Włochy
46. Zjednoczone Emiraty Arabskie