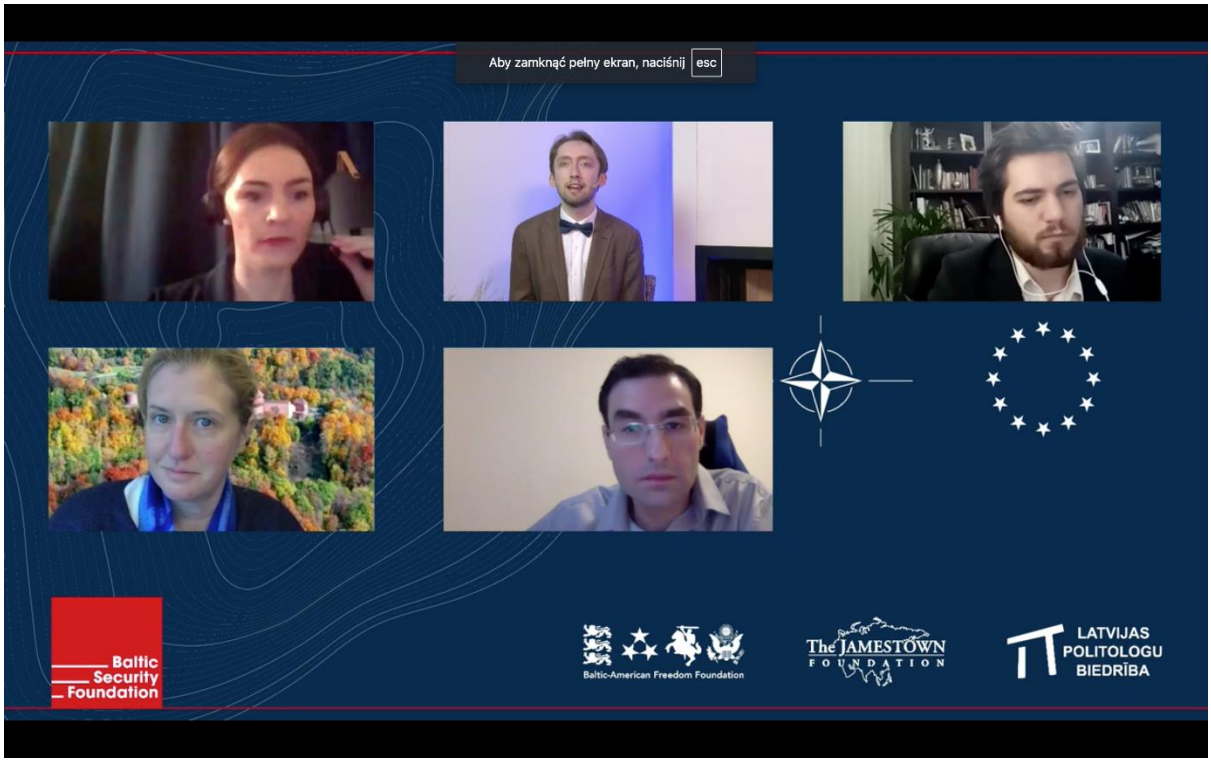
# Notatka z *Baltic Sea Security Conference: "Towards Coherent Strategy for the Region"*- cyberbezpieczeństwo

*Maria Piątek*

**04.12.2020**



**Notatka w skrócie:**

- W celu stworzenia bezpiecznej cyberprzestrzeni konieczna jest współpraca podmiotów międzynarodowych z sektorem prywatnym.
- Cyfryzacja ma coraz większy wpływ na organizację wyborów, dlatego trzeba zapewnić mechanizmy gwarantujące ich bezpieczne przeprowadzenie.
- Jednym z głównych niebezpieczeństw jest dezinformacja (fakenews, deepfake), która może kształtować opinie społeczeństw.

W czwartek, 3 grudnia 2020 r., w Helsinkach odbyła się konferencja „Towards a Coherent Strategy for the Region" organizowana przez Baltic Security Foundation, The Jamestown Foundation, Latvian Political Science Association i The Baltic-American Freedom Foundation.

W panelu dotyczącym cyberbezpieczeństwa wzięli udział: Peter Emoke z Komisji Europejskiej, który zajmuje się sprawami związanymi z wyborami oraz demokracją; Līga Rozentāle zajmująca się cyberbezpieczeństwem w Microsoft; Shota Gvineria, były ambasador Gruzji w Królestwie Niderlandów oraz wykładowca w Baltic Defence College; i Andreis Purim z Baltic Security Foundation. Debatę moderował Otto Tabuns z Baltic Security Foundation

**Peter Emoke** skupił się w swojej wypowiedzi na analizie dokumentów unijnych, których celem jest nawiązanie współpracy między państwami członkowskimi a Unią Europejską w sferze cyfryzacji oraz wypracowanie odpowiednich mechanizmów zapewniających przeprowadzenie bezpiecznych wyborów. Jednym z dokumentów wypracowanych przez Komisję Europejską jest *Report on the 2019 elections to the European Parliament*, według którego ostatnie wybory były najbardziej „cyfrowymi" w historii. Przyczyniło się do tego aktywne uczestnictwo dużej części społeczeństwa w cyberprzestrzeni, dzięki czemu kandydaci mogli podzielić swoimi ideami i pomysłami z większą grupą odbiorców. Według danych zaprezentowanych w raporcie prawie połowa obywateli UE czerpie wiedzę na temat polityki z internetu, jednak większość z nich uważa, że nie można takim informacjom ufać. **Wybory mogę stać się celem manipulacji innych podmiotów (zarówno państwowych jak i niepaństwowych), które w swoim działaniu będą korzystać z osiągnięć cyfryzacji.**

**Līga Rozentāle** zaznaczyła jak istotne jest uczestnictwo sektora prywatnego w dyskusji dotyczącej obrony i bezpieczeństwa cyberprzestrzeni oraz budowanie razem z rządami

nowych strategii w tym zakresie. Współpraca powinna bazować na fundamentalnych wartościach i zaufaniu. **Wiele organizacji międzynarodowych zajmuje się już tymi zagadnieniami i zaznacza rolę sektora prywatnego – jak np. NATO, które pod koniec listopada 2020 roku opublikowało dokument *NATO 2030: United for New Era - Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General,* w którym budowanie współpracy między sektorem prywatnym a państwami zostało kilkukrotnie wspomniane**. Z raportu Microsoft *Digital Defense Repor*t, który został opublikowany we wrześniu, wynika, że w przeciągu ostatniego roku metody, którymi posługują się napastnicy w cyberprzestrzeni stały się trudniejsze do wykrycia. Sprawcy przenoszą się do chmury, dzięki czemu łatwiej jest im się ukryć wśród legalnych usług. Celem ataku stają się nawet dobrze zabezpieczone systemy. Zauważalne jest większe zainteresowanie przestępców Internetem Rzeczy (IoT). Līga Rozentāle podkreśla, że Microsoft rocznie przeznacza duże środki pieniężne w celu walki z cyberatakami i cyberzagrożeniami. Firma ta skupia się również na działaniach politycznych i strategicznych. Jedną z najważniejszych inicjatyw jest współpraca z ponad tysiącem partnerów z dziedziny bezpieczeństwa i cyberprzestrzeni. Z zakresu bezpieczeństwa wyborów Microsoft pracuje nad oprogramowaniem EletionGuard, które ma zapewnić bezpieczeństwo procesu głosowania. Ma być ono użyte przy kolejnych wyborach prezydenckich w USA. **Ponadto Microsoft podejmuje działania z zakresu walki z dezinformacją w związku z czym zaprezentował Microsoft Video Authenticator.**

W swoim wystąpieniu Rozentāle przywołała również The Paris Call for Trust and Security z 12 listopada 2018, które zawiera wezwanie do wspólnego stawienia czoła nowym zagrożeniom. Zawiera 9 zasad, które dotyczą odpowiedzialnego zachowania w cyberprzestrzeni. Zwróciła ona także uwagę na obszar Morza Bałtyckiego – jest zdania, że dla tego regionu ważne jest istnienie ekosystemu zbudowanego na zaufaniu i stabilności w cyberprzestrzeni.

**Shota Gvineria** na początku zaznaczył, że **cyberprzestrzeń jest najważniejszym czynnikiem w środowisku bezpieczeństwa w XXI wieku.** Jego zdaniem nie można nie doceniać konwencjonalnych zagrożeń militarnych, jednakże w dzisiejszych czasach i na omawianym obszarze basenu Morza Bałtyckiego nie są one raczej prawdopodobne. **W przypadku konfliktu, Rosja stosowałaby raczej działania o charakterze hybrydowym**. **Cyberprzestrzeń umożliwia Rosjanom niekonwencjonalne działania,**

**dzięki którym osiągają swoje cele.** Aby zlikwidować zagrożenie, należy zrozumieć w jaki sposób odpowiednio zabezpieczyć cyberprzestrzeń. Z tego powodu obszar Morza Bałtyckiego potrzebuje spójnej polityki i strategii. Zdaniem ambasadora, kryzys związany z pandemią koronawirusa pokazał jak ważnym obszarem jest cyberprzestrzeń. Coraz więcej aspektów życia przenosi się do sieci i jest to tendencja, która przybiera na sile. Zauważa, że państwa bałtyckie zrobiły duży progres pod względem cyfryzacji – w szczególności zaś Estonia, która stworzyła rozbudowaną e-administrację.

Gvineria przywołał również wspomniany raport NATO, w którym zostało wskazane, że kluczowym priorytetem organizacji jest stworzenie wspólnych ram politycznych dotyczących oceny i reagowania na cyberataki.

Zdaniem **Andreisa Purima** istnieje dużo problemów związanych z cyberbezpieczeństwem, którym trzeba stawić czoła. W swojej wypowiedzi skupił się on na takich zagrożeniach jak fakenews i deepfake. Tworzone zabezpieczenia powinny chronić nie tylko kwestie techniczne, ale również instytucje i całe społeczeństwa. **Ludzie powinni mieć zaufanie do systemów, których używają, ale muszą mieć też świadomość, że niemożliwe jest stworzenie do końca bezpiecznego oprogramowania, bowiem każdy program może paść ofiarą cyberataku.**

Zwrócił uwagę, że w Europie zazwyczaj przekaz medialny jest rzetelny, niemniej jednak jako państwo często kreujące alternatywną wersję wydarzeń i szerzącą dezinformację wskazał Rosję. Jako przykład podał wydarzenia, które miały miejsce się na Ukrainie w 2014 i 2015 roku. W rosyjskich mediach społecznościowych (często na oficjalnych kontach rządowych) były prezentowane jako działania buntownicze i niewłaściwe. Jako kolejny problem wskazał zjawisko deepfake, polegające na manipulacji obrazem i głosem w taki sposób, że przedstawiona w filmie osoba wypowiada słowa oraz robi rzeczy, które nigdy nie miały miejsca. **Użytkownikom internetu brakuje krytycznego podejścia do treści zawartych w cyberprzestrzeni, dlatego mówiąc o niebezpieczeństwach wynikających z cyfryzacji, należy rozważyć wpływ, jaki dezinformacja może mieć na społeczeństwa.**

## O AUTORCE

**Maria Piątek**. Absolwentka studiów licencjackich na kierunku europeistyka w Centrum Europejskim UW oraz studentka III roku prawa na UW. Zainteresowania dotyczą m.in. procesów integracyjnych i dezintegracyjnych w Europie, dyplomacji, rozwoju technologicznego oraz geopolityki.

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018 – 2030

**JEŻELI DOCENIASZ NASZĄ PRACĘ, DOŁĄCZ DO GRONA NASZYCH DARCZYŃCÓW!**

Z otrzymanych funduszy sfinansujemy powstanie kolejnych publikacji.

Możliwość wsparcia to bezpośrednia wpłata na konto Instytutu Nowej Europy: 95 2530 0008 2090 1053 7214 0001 tytułem: „darowizna na cele statutowe”.