Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje

Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska, Jozef Vyskoč, Maciej Ziarek
Redakcja: Joanna Świątkowska

Visegrad Fund

Instytut Kościuszki

Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje

Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska,
Jozef Vyskoč, Maciej Ziarek
Redakcja: Joanna Świątkowska

Visegrad Fund

Instytut Kościuszki

Jeżeli doceniają Państwo wartość merytoryczną niniejszej publikacji, zachęcamy do finansowego wsparcia przyszłych inicjatyw wydawniczych Instytutu.

Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje

Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska, Jozef Vyskoč, Maciej Ziarek
Redakcja: Joanna Świątkowska

Publikacja współfinansowana przez
Międzynarodowy Fundusz Wyszehradzki
(http://visegradfound.org)

Visegrad Fund

Tłumaczenie: Karolina Gucko (rozdz. 3, 6), Renata Lasota (rozdz. 5), Bartosz Wójcik (rozdz. 7).

Pomoc w edycji: Bartosz Wójcik, Karolina Gucko

Projekt i skład graficzny: Małgorzata Kopecka
Druk: Dante Media

Instytut Kościuszki
ul. Lenartowicza 7/4
31-138 Kraków
e-mail: ik@ik.org.pl
+48 12 632 97 24
www.ik.org.pl

ISBN: 978-83-63712-06-8

Spis treści

Nie wszystkie opinie wyrażone w niniejszej publikacji przez jej autorów odzwierciedlają oficjalne stanowisko programowe Instytutu Kościuszki oraz partnerów publikacji. Stanowią one wkład w debatę publiczną. Tezy zawarte w publikacji odzwierciedlają stanowiska poszczególnych autorów, niekoniecznie stanowiąc opinie pozostałych.

Wstęp

Izabela Albrycht – prezes zarządu Instytutu Kościuszki

Rozwiązania teleinformatyczne wpływają na każdą sferę życia publicznego i prywatnego, a także są odpowiedzialne za prawidłowe funkcjonowanie państw współczesnych. Z jednej strony postęp technologiczny umożliwił niespotykany wcześniej rozwój cywilizacyjny, z drugiej jednak strony doprowadził do wyłonienia nowych zagrożeń, które muszą stać się przedmiotem działań i decyzji podmiotów odpowiedzialnych za sferę bezpieczeństwa.

Cyberbezpieczeństwo nie zna granic – rozwiązania wyłącznie na poziomie państwowym nie są wystarczające. Aby sprostać cyberzagrożeniom konieczna jest międzynarodowa współpraca, a sojusze regionalne takie jak Grupa Wyszehradzka, stanowią kluczowy komponent, a zarazem dopełnienie wielostronnej współpracy.

Głównym celem niniejszej publikacji jest dokonanie analizy stanu cyberbezpieczeństwa w państwach Grupy Wyszehradzkiej oraz przedstawienie rekomendacji służących jego wzmacnianiu. Czechy, Słowacja, Węgry oraz Polska są członkami Unii Europejskiej oraz NATO. Oba te podmioty wzbogaciły swoją agendę o działania z zakresu ochrony cyberprzestrzeni. Publikacja zawiera nie tylko analizę działań podejmowanych przez NATO i UE w tej sferze, ale także prezentuje możliwe obszary solidarnych działań państw Grupy Wyszehradzkiej, służących dalszemu umacnianiu cyberbezpieczeństwa na arenie międzynarodowej także w ramach tych organizacji.

Jednym z istotnych celów publikacji jest także przybliżenie czytelnikowi podstawowych informacji z zakresu ochrony cyberprzestrzeni i uświadomienie jak bardzo istotny jest to obszar z punktu widzenia bezpieczeństwa każdego obywatela. Społeczna świadomość zagrożeń jest niezwykle ważnym elementem prewencji w obliczu globalizacji zagrożeń cybernetycznych.

Publikacja z racji swoich parametrów omawia najważniejsze zagadnienia związane z cyberbezpieczeństwem. Każdy z niniejszych rozdziałów stanowi punkt wyjścia do dalszych kompleksowych analiz, niemniej jednak stanowi solidną porcję wiedzy dla wszystkich zainteresowanych tematyką i problemami współczesnego bezpieczeństwa międzynarodowego.

Wszystkie analizy oparte zostały o informacje jawne i skupiają się na nietechnicznych aspektach obrony cyberprzestrzeni. Zaletą takiego podejścia jest przystępność tekstu i możliwość uchwycenia politologicznego wymiaru problemu cyberbezpieczeństwa. Z uwagi na taką perspektywę publikacja stanowi wartościowy i użyteczny materiał dla decydentów, którzy w oparciu o jej rekomendacje mogą adresować odpowiednie rozwiązania polityczne – zarówno krajowe jak i międzynarodowe. Raport jest również źródłem praktycznej wiedzy dla wszystkich zainteresowanych nowymi trendami w sferze bezpieczeństwa międzynarodowego.

Dziękując naszym Partnerom za współpracę przy realizacji raportu, zapraszam Państwa do jego lektury, a także podjęcia dyskusji na temat kwestii cyberbezpieczeństwa, które stać się musi, obok bezpieczeństwa ekonomicznego, energetycznego i militarnego, kluczowym komponentem strategii bezpieczeństwa tak poszczególnych krajów, jak i naszej „globalnej wioski".

Wybrane tezy*

Instytut Kościuszki

Zagrożenia cyberprzestrzeni wyzwaniem dla bezpieczeństwa współczesnego świata
Autor: Joanna Świątkowska
Żyjemy w świecie, w którym funkcjonowanie a także rozwój jednostek, państw oraz organizacji międzynarodowych opiera się na wykorzystaniu rozwiązań teleinformatycznych. W wyniku rozwoju technologicznego, obok niebagatelnych korzyści, pojawiły się nowe typy zagrożeń, którym społeczność międzynarodowa musi stawić czoła. Jednym z najważniejszych wyzwań, jakie stoi przed państwami oraz innymi podmiotami jest zapewnienie bezpieczeństwa cyberprzestrzeni.

Zagrożenia cyberprzestrzeni zrewolucjonizowały myślenie o bezpieczeństwie, zburzyły stare paradygmaty dotyczące metod jego zapewniania i reguł związanych z międzynarodowym konfliktem.

Do głównych niebezpieczeństw związanych z użytkowaniem cyberprzestrzeni należy: cyberprzestępstwo, cyberterroryzm oraz cyberwojna.

Problemy wyżej opisane mogą zostać przezwyciężone wyłącznie dzięki współpracy międzynarodowej i międzysektorowej. (…) Jednym z celów tej publikacji jest zwrócenie uwagi, że cyberbezpieczeństwo powinno być wspólnym celem także działań państw Grupy Wyszehradzkiej.

Systematyzacja największych cyberzagrożeń
Autor: Maciej Ziarek
Od kiedy Internet stał się medium wykorzystywanym w każdej niemal dziedzinie życia, wzrasta ryzyko wykorzystania go przez cyberprzestępców do ataków i nielegalnych zysków. (…) Szkodliwe oprogramowanie w wersji na tradycyjne systemy, w wersji na systemy mobilne, spam czy botnety to realia współczesnego Internetu.

Botnety (…) są tworzone przez sieć zainfekowanych komputerów, których właściciele nie zdają sobie z tego sprawy. Tak zainfekowany komputer potocznie określa się mianem maszyny zombie. (…) Jego użycie jest zależne od intencji autora, czyli cyberprzestępcy.