Marek Górka, *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013-2017*, Wydawnictwo Difin, Warszawa 2019, ss. 340

(Marcin Adamczyk)

O wadze zagadnienia, jakim jest cyberbezpieczeństwo nie trzeba chyba w XXI w. nikogo przekonywać – znajduje to swoje odbicie w rosnącej ilości konferencji, artykułów czy całych monografii poświęconych tej problematyce. W trend ten wpisuje się również najnowsza książka Marka Górki z Politechniki Koszalińskiej, młodego, ale i uznanego badacza w tym obszarze. Nie jest to bynajmniej ujma dla autora, że wybiera temat „na topie" – ważnym jest, aby podejmowany w pracy problem badawczy był świeży, co niewątpliwie się Górce udało osiągnąć. Choć przyjęte cezury czasowe w książce mogą z początku nieco konfundować, to jednak autor wyczerpująco uzasadnia przyczynę określenia takich właśnie ram dla przeprowadzonych badań. Relatywnie krótki okres poddany analizie nie wpłynął zasadniczo na objętość monografii, która liczy sobie przyzwoite trzy i pół setki stron – dobrze, że autor nie postanowił ulec modzie na tworzenie monumentalnych publikacji liczących po 600 i więcej stron, które być może dobrze wyglądają w dorobku naukowym i czasem również na półce w bibliotece, ale niekoniecznie nadają się do czytania. Książka składa się z pięciu rozdziałów (zatytułowanych odpowiednio: *Bezpieczeństwo cybernetyczne w przestrzeni politycznej UE i NATO*, *Uwarunkowania cybernetyczne i pozacybernetyczne państw Grupy Wyszehradzkiej*, *Cyberzagrożenia jako czynniki kształtujące politykę państw Grupy Wyszehradzkiej*, *Technologie informacyjno-komunikacyjne w polityce cyberbezpieczeństwa państw Grupy Wyszehradzkiej*, *Perspektywy polityki cyberbezpieczeństwa państw Grupy Wyszehradzkiej*), wstępu i zakończenia oraz aneksów w postaci tabel zawierających szereg danych statystycznych, które tematycznie oscylują wokół głównego problemu poruszanego w książce. Ponadto autor umieścił w swojej publikacji równie nieodzowny wykaz skrótów oraz krótkie streszczenie w języku angielskim (sens tego ostatniego wydaje się dyskusyjny, ale prawo piszącego umieścić w swoim dziele wszystko to, na co ma ochotę) i rzecz jasna, bibliografię (podzieloną na kilka kategorii i liczącą blisko pół tysiąca pozycji).

Wstęp stanowi kompleksowe i wyczerpujące wprowadzenie do pracy – autor definiuje w nim najważniejsze pojęcia, uzasadnia wybór przyjętych ram czasowych, prezentuje postawione w swojej pracy cele, pytania i hipotezy badawcze,

wykorzystane metody, odnosi się on także do aktualnego stanu badań i wykorzystanego materiału badawczego oraz zapoznaje czytelnika z treścią kolejnych rozdziałów. Nie można raczej nic zarzucić wobec tak przygotowanego wstępu – można by jedynie się zastanowić czy nie warto bardziej podkreślić (poprzez wprowadzenie podrozdziałów) odrębności poszczególnych jego elementów. Z drugiej strony sam fakt, że autor swój wstęp odpowiednio ustrukturyzował – nie tylko wpływa to na jasność wywodu, ale znacznie ułatwia lekturę. Warto nadmienić, iż sprecyzowane cele badawcze są jak najbardziej poprawne, a sformułowane hipotezy wynikają z postawionych pytań. Dobór materiału badawczego jest właściwy i sprowadza się właściwie do dwóch kategorii, czyli opracowań naukowych i dokumentów oraz oficjalnych raportów. Interesującym zabiegiem (z punktu widzenia tematyki niewątpliwie koniecznym) było wykorzystanie wywiadów z ekspertami. Jedyne czego może brakować we wstępie to bardziej rozwinięty wątek motywacji autora do podjęcia akurat tych badań.

Rozdział pierwszy zatytułowany *Bezpieczeństwo cybernetyczne w przestrzeni politycznej UE i NATO* składa się z trzech podrozdziałów, z których drugi i trzeci zostały podzielone na kolejne (odpowiednio cztery i pięć paragrafów). Autor skupia się w nim na działaniach mających na celu włączenie problemu cyberbezpieczeństwa do agendy obu organizacji oraz ich sprawności w radzeniu sobie z cyberzagrożeniami w kontekście ewolucji cyberbezpieczeństwa. Przyjętą formułę należy ocenić pozytywnie, choć podrozdział poświęcony ewolucji samego pojmowania cyberbezpieczeństwa mógłby równie dobrze znaleźć się we wstępie i tam dobrze wprowadzałby czytelnika w badane zagadnienie.

Rozdział drugi pt. *Uwarunkowania cybernetyczne i pozacybernetyczne państw Grupy Wyszehradzkiej* to z jednej strony niezbyt długa, choć na potrzeby niniejszej monografii raczej wystarczająca, historia powstania i funkcjonowania grupy V4 oraz wprowadzenie do polityki cyberbezpieczeństwa członków grupy (ten podrozdział został podzielony na trzy części poświęcone odpowiednio deklaracjom politycznym, formułowanym strategiom oraz wydatkom na bezpieczeństwo cybernetyczne).

Jest oczywiste, że najważniejszą część pracy stanowią rozdziały trzeci (*Cyberzagrożenia jako czynniki kształtujące politykę państw Grupy Wyszehradzkiej*) oraz czwarty (*Technologie informacyjno-komunikacyjne w polityce cyberbezpieczeństwa państw Grupy Wyszehradzkiej*). Pierwszy z nich poświęcony jest cyberatakom i próbom siania dezinformacji w cyberprzestrzeni wymierzonym w państwa grupy V4 oraz wysiłkom na rzecz przeciwdziałania tym zjawiskom. Warto w tym kontekście docenić niepominięcie przez autora ważnego w tym kontekście problemu *fake newsów* (choć wątek ten mógłby zostać bardziej rozwinięty). Interesująca jest teza postawiona przez autora na początku rozdziału, zakładająca, iż zachodzi korelacja pomiędzy incydentami w cyberprzestrzeni, a pozycją międzynarodową państw Grupy Wyszehradzkiej.

Drugi ze wspomnianych rozdziałów poświęcony jest wykorzystaniu ICT w państwach Wyszehradu na tle innych regionów europejskich – niestety, wnioski z lektury tegoż rozdziału nie są optymistyczne i stoją w sprzeczności z pokutującym mitem naszego państwa jako zagłębia informatycznego. Niemniej jest to wartościowa analiza, nawet jeżeli o gorzkim wydźwięku.

Autora niniejszej recenzji szczególnie natomiast zainteresował rozdział ostatni, którego tytuł *Perspektywy polityki cyberbezpieczeństwa państw Grupy Wyszehradzkiej* obiecuje znacznie mniej niż czytelnik rzeczywiście otrzymuje (co zdarza się rzadko, gdyż zazwyczaj zachodzi sytuacja zgoła odwrotna). Marek Górka nie tylko pokazuje potencjalne kierunki rozwoju tytułowej polityki cyberbezpieczeństwa, ale również zestawia ze sobą obowiązujące strategie cyberbezpieczeństwa w Polsce i Czechach oraz na Słowacji i Węgrzech (ten fragment również w odczuciu autora mógłby znaleźć się w innej części książki), przede wszystkim jednak analizuje on związki między demokracją a cyberbezpieczeństwem i zestawia grupę V4 z Chinami, Rosją oraz USA – szkoda, że autor tego wątku nie rozwinął bardziej, np. tworząc z niego osobny rozdział. Praca kończy się kilkustronicowym podsumowaniem, wobec którego nie można mieć żadnych zarzutów, gdyż autor trafnie podsumowuje swoje badania odnosząc się do każdej hipotezy z osobna – co niewątpliwie wpływa pozytywnie na czytelność pracy i dobrze świadczy o podejściu badacza do własnej pracy naukowej.

Jak już wspomniano na wstępie, recenzowana książka Marka Górki wpisuje się w popularny w ostatnich latach nurt badań nad cyberbezpieczeństwem, a jednocześnie podejmuje zagadnienie nowe z punktu widzenia obecnego stanu nauki. Nie da się ukryć, że większość prac poświęconych jest „wielkim tego świata", co nie dziwi, biorąc pod uwagę rosnącą temperaturę sporu chińsko-amerykańskiego czy zagrożenie ze strony Rosji. Cieszy fakt, że autor postanowił się zająć relatywnie mało modną w tym kontekście Grupą Wyszehradzką. Być może należałoby w większym stopniu odnieść się do kontekstu międzynarodowego (nie tylko wobec UE i NATO, ale również wspomnianej rywalizacji USA, Chin i Rosji) czy inaczej rozłożyć niektóre podrozdziały, nie zmienia to jednak faktu, iż monografia *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013-2017* to kawał dobrej naukowej roboty, która zasługuje na polecenie wszystkim zainteresowanym politycznymi aspektami cyberbezpieczeństwa w naszym regionie.