AUTOREFERAT

1. IMIĘ I NAZWISKO: Marek Leszek Górka

2. POSIADANE DYPLOMY, STOPNIE NAUKOWE

W 1997 roku podjąłem stacjonarne studia licencjackie na kierunku polonistyka (specjalność: nauczycielska) na Wydziale Humanistycznym Uniwersytetu Szczecińskiego. Studia te ukończyłem w roku 2000 z wynikiem końcowym bardzo dobrym.

Bezpośrednio po ukończeniu studiów licencjackich rozpocząłem pięcioletnie studia magisterskie na kierunku politologia na Wydziale Humanistycznym Uniwersytetu Mikołaja Kopernika w Toruniu, które ukończyłem z wynikiem dobrym plus w 2005 roku.

Podczas studiów w 2004 roku ukończyłem dodatkowo dwuletnie Europejskie Studia im. Jana Moneta na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu.

W 2007 roku rozpocząłem studia doktoranckie na Wydziale Nauk Politycznych na Akademii Humanistycznej im. Aleksandra Gieysztora w Pułtusku. Stopień doktora nauk humanistycznych w zakresie nauk o polityce uzyskałem na podstawie decyzji Rady Wydziału Nauk Politycznych Akademii Humanistycznej im. Aleksandra Gieysztora w Pułtusku w dniu 10 października 2011 roku, po publicznej obronie rozprawy doktorskiej pt. *Wybory parlamentarne w Polsce w 2007 roku. Uwarunkowania, przebieg i konsekwencje polityczne*. Promotorem pracy był prof. dr hab. Mirosław Chałubiński.

3. INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH

Od 1 października 2010 roku byłem zatrudniony na stanowisku asystenta w ówczesnym Instytucie Polityki Społecznej i Stosunków Międzynarodowych na Politechnice Koszalińskiej.

Z dniem 1 października 2015 roku zostałem mianowany na stanowisko adiunkta. Politechnika Koszalińska jest moim podstawowym miejscem pracy. W wyniku zmian w strukturze organizacyjnej Instytutu Polityki Społecznej i Stosunków Międzynarodowych Politechniki Koszalińskiej, w październiku 2015 roku zostałem pracownikiem Wydziału Humanistycznego.

4. Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U. z 2017 r. poz. 1789)

a) tytuł osiągnięcia naukowego, rok wydania, nazwa wydawnictwa

Monografia, którą pragnę przedstawić zgodnie z wymaganiami art. 16 ust. 2 ustawy z 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U. z 2016 r. poz. 882 ze zm. w Dz.U. z 2016 r. poz. 1311) jako osiągnięcie naukowe, uzyskane po otrzymaniu stopnia doktora, stanowiące znaczny wkład w rozwój określonej dyscypliny naukowej, jest publikacją mojego autorstwa zatytułowaną: *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*. Książka została opublikowana w 2019 roku nakładem Wydawnictwa Difin, ss. 336 (ISBN: 978-83-8085-868-8).

b) autor/autorzy, tytuł/tytuły publikacji, rok wydania, nazwa wydawnictwa, recenzenci wydawniczy

Marek Górka, *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017,* Warszawa 2019, Wydawnictwo Difin, ss. 336 (ISBN: 978-83-8085-868-8).

Recenzenci:

- dr hab. Izabela Oleksiewicz, profesor Politechniki Rzeszowskiej;
- prof. dr hab. Jacek Knopek, Uniwersytet Mikołaja Kopernika w Toruniu.

c) przedstawienie celu naukowego ww. pracy i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

Przedstawiona do oceny monografia poświęcona jest analizie doświadczeń państw Grupy Wyszehradzkiej w obszarze polityki bezpieczeństwa cybernetycznego w okresie 2013–2017. Problem omawiany w pracy, dotyczący cyberbezpieczeństwa, postrzegany jest z perspektywy nauk o polityce, jednocześnie jednak dotyczy wieloaspektowego charakteru działań państwa, na który składają się czynniki polityczne, gospodarcze, społeczne oraz kulturowe. Praca ma dowieść, że cyberbezpieczeństwo nie jest jedynie domeną technologii, bowiem to wyżej wspomniane aspekty w znacznie bardziej zdecydowany sposób kształtują warunki stabilnego

rozwoju państwa i jego obywateli w przestrzeni zdominowanej przez cybertechnologię. Drugą ważną częścią tematu badawczego pracy są państwa Grupy Wyszehradzkiej, które podobnie jak inne państwa na świecie poddane były – i nadal są – procesom wynikającym z upowszechnienia cyberprzestrzeni.

Dowody na rosnące znaczenie cyberbezpieczeństwa dostrzegalne są już od wielu lat, a ich symbolicznym momentem były wydarzenia w Estonii w 2007 roku, w Gruzji w 2008 roku czy też w Iranie w 2010 roku. Incydenty te uświadomiły skalę zagrożeń oraz wyzwań, z jakimi muszą zmierzyć się rządy wielu państw. Rosnąca rola cybertechnologii prawie we wszystkich dziedzinach ludzkiego życia zmusza i inspiruje badaczy również do stawiania pytań o naturę współczesnej polityki. Co więcej, znaczna część cyberincydentów – jak wskazano w pracy –motywowana jest ideologicznie, a za wieloma tego typu wydarzeniami stoją państwa lub podmioty działające w ich interesie, co jest kolejnym powodem zajęcia się tym tematem z perspektywy nauk o polityce.

Z jednej strony pojawiające się zagrożenia cybernetyczne ukazują słabość państwa oraz zależność instytucji państwowych od cybertechnologii, z drugiej jednak – zaistniałe cyberincydenty mogą motywować rządy wielu państw do podjęcia działań w celu zwiększenia poziomu bezpieczeństwa cybernetycznego. Uwaga ta stała się dodatkowym czynnikiem motywującym do podjęcia analizy polityki bezpieczeństwa cybernetycznego państw Grupy Wyszehradzkiej.

Temat dotyczący zjawisk zachodzących między cyberprzestrzenią i polityką państw V4 nie doczekał się jeszcze syntetycznego ujęcia w literaturze przedmiotu. Wcześniejsze publikacje w dość ograniczony sposób przedstawiały problem cyberbezpieczeństwa państw V4, skupiając uwagę na dotychczasowych doświadczeniach w zakresie współpracy politycznej oraz w kontekście transformacji ustrojowej regionu Europy Środkowej. Z pewnością wynika to m.in. z tego powodu, że cyberzagrożenia są wciąż dość nowym zjawiskiem. Dlatego też celem prezentowanej monografii jest wypełnienie tej luki badawczej oraz zabranie głosu w toczącej się dyskusji na temat zachodzących przemian inicjowanych przez wzrost znaczenia cybertechnologii we współczesnej polityce.

Monografia obejmuje przedział czasowy 2013–2017. Jednakże ze względu na potrzebę wyjaśnienia genezy oraz przyczyn określonych procesów analiza badawcza wykracza poza wyznaczoną cezurę. Rok 2013 można uznać za nowy etap kształtowania cyberbezpieczeństwa w obszarze UE, w tym czasie bowiem wprowadzono *Strategię bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, która to w dużym stopniu stała się czynnikiem determinującym politykę państw członkowskich w

obszarze cyberbezpieczeństwa. Ponadto w tym samym roku utworzone zostało (w ramach Europolu) Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), zajmujące się zwalczaniem cyberprzestępczości.

Na uwagę zasługują również procesy, które zachodzą poza granicami UE i którym towarzyszą zjawiska o naturze cyfrowej. Przykładem tego jest przede wszystkim konflikt na wschodzie Ukrainy, który rozgrywa się m.in. przy wykorzystaniu nowych technologii cyfrowych. Zjawisko to jest jednym z czynników, które wpłynęły na zmianę postrzegania natury współczesnych zagrożeń, zmuszając w ten sposób część państw członkowskich UE do zmiany dotychczasowej polityki bezpieczeństwa cybernetycznego.

Wzrost zagrożeń został dostrzeżony przez środowiska polityczne wielu państw europejskich, w związku z czym pojawiła się coraz silniejsza potrzeba zmian w zakresie cyberprzestrzeni. Dowodem tego stało się wprowadzenie dwóch nowych aktów prawnych, tj. *Dyrektywy w sprawie bezpieczeństwa sieci i informacji* (NIS) oraz *Ogólnego rozporządzenia o ochronie danych* (GDPR), które obecnie kształtują podstawowe ramy europejskiego bezpieczeństwa cybernetycznego w wymiarze społeczno-gospodarczym. Ponadto zmiany dotyczyły odnowienia dotychczasowej strategii cyberbezpieczeństwa z 2013 roku, wprowadzono również europejski system certyfikacji, zainicjowano budowę wspólnego rynku cyfrowego oraz poszerzono uprawnienia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). Powyższe zmiany w znacznym stopniu zaczęto realizować w 2016 i 2017 roku, dlatego też stanowią one w pracy klamrę zamykającą analizowany przedział czasowy.

W kontekście analizowanego tematu wykorzystana jest koncepcja europeizacji, która okazuje się użyteczna dla analizy polityki bezpieczeństwa cybernetycznego państw Grupy Wyszehradzkiej. W tym podejściu traktowana jest ona jako proces opisujący zmiany wewnętrzne spowodowane wpływem generowanym przez UE. Skutkiem europeizacji jest więc adaptacja wymagań europejskich na poziomie państwa. Proces ten nie oznacza jednak w prosty sposób ujednolicenia norm i zasad ponad granicami, ponieważ różnice w polityce i kulturze poszczególnych państw prowadzą do różnych wyników, które są efektem dostosowań tych samych zasad generowanych przez UE. Na przykład, dyrektywa NIS jest różnie interpretowana w poszczególnych państwach, w zależności od odmiennego systemu administracyjnego, kultury politycznej czy choćby oczekiwań społecznych. A zatem proces adaptacji zależy od państwa. Ponadto istnieje wiele czynników, które mogą mieć wpływ na stopień zachodzących zmian. Należy się zatem spodziewać, że uzyskanie identycznych wyników w regionie Europy Środkowej jest niemożliwe. Dlatego też polityka

cyberbezpieczeństwa prowadzona w państwach V4 okazuje się intrygującym wyzwaniem badawczym, wnoszącym nowy wkład w dotychczasowy obszar wiedzy na temat państw Grupy Wyszehradzkiej.

Ważnym wyzwaniem w pracy jest pomiar polityki cyberbezpieczeństwa, realizowany za pomocą danych pochodzących z różnych źródeł i jednocześnie odzwierciedlających odmienne uwarunkowania polityczne, gospodarcze i społeczne badanych regionów. Monografia powstała na podstawie oficjalnych raportów przygotowanych przez Komisję Europejską oraz międzynarodowe organizacje pozarządowe, ilustrujących m.in. stopień rozwoju gospodarki cyfrowej, poziom finansów publicznych, skalę cyberzagrożeń oraz poziom demokracji i wolności słowa. Wykorzystano również dane na temat funkcjonowania społeczeństwa i przedsiębiorstw w kontekście nowych technologii. W celu scharakteryzowania oficjalnych stanowisk zajmowanych przez rządy państw Grupy Wyszehradzkiej uwzględniono także dokumenty strategiczne – w tym UE i NATO – odwołujące się do bezpieczeństwa cybernetycznego.

Aby jednak w pełni zilustrować rolę i znaczenie cyberprzestrzeni w polityce bezpieczeństwa państw Grupy Wyszehradzkiej, której natura w dużym stopniu jest trudna do uchwycenia i odbiega od tradycyjnych wymiarów polityki, wykorzystano informacje pozyskane w ramach uczestnictwa w międzynarodowym projekcie pod tytułem „Visegrad Group and the Central European Cooperation" (No. 61450025) finansowanym przez Międzynarodowy Fundusz Wyszehradzki. Dzięki spotkaniom z badaczami zajmującymi się polityką bezpieczeństwa oraz osobami związanymi z praktycznym wymiarem w tej dziedzinie możliwe stało się pozyskanie odpowiednich danych ilustrujących m.in. wydatki na poprawę cyberbezpieczeństwa oraz skalę przeprowadzonych cyberataków wobec państw V4, co umożliwiło poszerzenie wiedzy o informacje dotąd niepublikowane. W wyniku tego dokonano porównania i skonfrontowania oficjalnych danych z wiedzą o charakterze poufnym.

Drugim ważnym wydarzeniem pozwalającym pozyskać informacje na temat zaistniałych cyberincydentów w państwach V4 była Międzynarodowa Konferencja „Medea 2017" odbywająca się na Uniwersytecie Kreteńskim Heraklion w Grecji w dniach 1–8 września 2017 roku. Uczestnictwo w tym wydarzeniu stało się okazją do przeprowadzenia bezpośredniego wywiadu z pracownikami ENISA oraz pozyskania danych, do których dostęp jest utrudniony z racji ich poufnego charakteru, a które pozwalają znacznie dokładniej zmierzyć, scharakteryzować oraz ocenić dotychczasowe działania państw europejskich.

Polityka bezpieczeństwa cybernetycznego definiowana jest w monografii w dwóch perspektywach. Pierwsza odnosi się do umiejętności korzystania z cyberprzestrzeni w celu

tworzenia korzystnych instrumentów władzy i realizowania zadań w wybranych obszarach przez państwo. To spojrzenie odnosi się szczególnie do wymiaru międzynarodowego, w którym państwa wykorzystują cyberprzestrzeń jako narzędzie wpływu i wywierania presji na inne podmioty.

Drugie podejście interpretuje to pojęcie jako przestrzeń licznych komplementarnych oraz konkurencyjnych procesów wynikających z czynników wewnętrznych wpływających na innowacyjność w obszarze gospodarki cyfrowej (jak m.in. rozwój ICT, wzrost nakładów na badania i rozwój, liczba petentów itp.). Na poziomie państwa funkcjonowanie polityki cyberbezpieczeństwa może być uzależnione od innych przyczyn, takich jak: zmiany polityczne w wyniku wyborów, wpływ grup nacisku lub też nastroje i oczekiwania społeczne będące pokłosiem innych wydarzeń politycznych. A zatem wszystkie te czynniki składają się na szerokie spektrum definicji polityki cyberbezpieczeństwa.

W pracy poddano również weryfikacji hipotezę, iż oba te determinanty wewnętrzne, jak i zewnętrzne są od siebie wzajemnie zależne. Rozwój ICT jest ściśle związany z potencjałem gospodarczym państwa, co przekłada się także na jego znaczenie na arenie międzynarodowej.

Głównym celem badawczym niniejszej pracy jest analiza różnorodnych aspektów polityki cyberbezpieczeństwa członków Grupy Wyszehradzkiej ze szczególnym uwzględnieniem lat 2013–2017 i ich funkcjonowania w ramach UE i NATO. Na podstawie podjętej refleksji naukowej wyznaczono cztery dodatkowe cele badawcze, polegające na zbadaniu:

1) jakie są podobieństwa i różnice w definiowaniu oraz prowadzeniu polityki cyberbezpieczeństwa i czy odmienna interpretacja w tym obszarze może stanowić potencjalną kwestię sporną wśród członków Grupy Wyszehradzkiej;
2) w których obszarach cyberbezpieczeństwa członkowie Grupy Wyszehradzkiej odnieśli pozytywny skutek, a w których nie osiągnięto wyznaczonych celów i pozostają one w dalszym ciągu wyzwaniem, przed którym stoją te państwa;
3) jak można scharakteryzować i zrozumieć ewolucję polityki cyberbezpieczeństwa państw V4 wobec możliwych cyberzagrożeń;
4) w jakim stopniu państwa Grupy Wyszehradzkiej budują kompleksowe podejście do bezpieczeństwa cybernetycznego w otoczeniu politycznym i jakie są warunki niezbędne do zapewnienia skutecznego bezpieczeństwa.

W poszukiwaniu odpowiedzi na postawione powyżej cele sformułowano następujące hipotezy badawcze:

W nawiązaniu do pierwszego punktu skonstruowano hipotezę, zgodnie z którą identyfikacja podobieństw i różnic na poziomie polityki cyberbezpieczeństwa państw Grupy

Wyszehradzkiej przebiega w dwóch wymiarach: pierwszy dotyczy warstwy teoretycznej, drugi zaś działań praktycznych. Okazuje się zatem, że w warstwie artykułowanych celów politycznych zapisanych w dokumentach strategicznych i w deklaracjach z oficjalnych spotkań międzynarodowych oraz w programach prezydencji Grupy Wyszehradzkiej, poszczególne rządy mają tendencję do podobnego postrzegania wyzwań cybernetycznych jako zagrożeń dla prawidłowego funkcjonowania państwa. Jednakże istnieją również znaczne różnice. Odmienna perspektywa interpretacji cyberbezpieczeństwa zachodzi w wymiarze praktycznym, a szczególnie w zakresie wysokości wydatków budżetowych przeznaczanych na inwestycje w celu poprawy funkcjonowania ICT oraz działań innowacyjnych w ramach funkcjonowania infrastruktury krytycznej, a także zastosowań nowych technologii w obszarze umiejętności społecznych.

W związku z drugim pytaniem badawczym sformułowano hipotezę, że do najważniejszych elementów decydujących o rozwoju i potencjale państwa w zakresie polityki cyberbezpieczeństwa zalicza się rozwój gospodarki cyfrowej. Państwa Grupy Wyszehradzkiej starają się sprostać temu zadaniu, jednak ich działania w dużej mierze zależą od własnych możliwości i chęci rozwoju w poszczególnych sektorach. Analiza ewolucji polityczno-gospodarczej z udziałem technologii cyfrowej prowokuje także do postawienia dwóch kolejnych hipotez. Pierwsza dotyczy przypuszczenia, że odmienność i zróżnicowanie doświadczeń gospodarczych przebiega wzdłuż granic rozwoju cybertechnologii wśród państw europejskich. Druga z kolei hipoteza wskazuje na prawdopodobny związek pomiędzy znaczeniem państwa na arenie międzynarodowej a osiąganymi wynikami w zakresie innowacji oraz poziomem nakładów finansowych przeznaczanych na badania i rozwój cybertechnologii.

Odpowiadając na trzecie pytanie, hipoteza badawcza zakłada, iż najważniejszym czynnikiem determinującym politykę cyberbezpieczeństwa państw V4 jest przynależność do Unii Europejskiej i NATO. Innym ważnym aspektem kształtującym decyzje polityczne oraz wymiar bezpieczeństwa jest również stosunek do polityki rosyjskiej, który wśród państw V4 jest niejednoznaczny i w dużym stopniu zakłóca spójność polityczną w tym regionie Europy. Powiązane z tą hipotezą jest kolejne przypuszczenie dotyczące tego, że samo już zaistnienie cyberincydentów bądź możliwość ich wystąpienia może być czynnikiem wpływającym na politykę bezpieczeństwa cybernetycznego w wymiarze międzynarodowym.

W nawiązaniu do czwartego pytania hipoteza badawcza odnosi się do sposobu prowadzenia działań w zakresie cyberbezpieczeństwa przez państwa V4, który determinowany jest przynależnością do UE bądź NATO. Konsekwencją tak przyjętej

perspektywy przez środowiska polityczne państw V4 są postawy, decyzje i działania polityczne widoczne choćby w strukturze wydatków na cyberbezpieczeństwo, w akcentowaniu priorytetów politycznych zapisanych m.in. w dokumentach strategicznych. Innymi słowy, model polityki o charakterze cywilnej (bliskiej UE) czy też militarnej (odpowiadającej perspektywie NATO) koresponduje z podziałem na postawę „atlantyzmu" bądź „kontynentalizmu" na gruncie polityki cyberbezpieczeństwa państw Grupy Wyszehradzkiej.

Aby odpowiedzieć na powyższe pytania i zweryfikować hipotezy, zastosowane zostały metody badawcze. Ważną rolę, zwłaszcza w kontekście zidentyfikowanych różnic pomiędzy państwami V4 w polityce cyberbezpieczeństwa, odgrywa metoda porównawcza (komparatystyczna). Poprzez odnotowanie zachodzących podobieństw i różnic pomiędzy członkami Grupy Wyszehradzkiej możliwe stało się scharakteryzowanie funkcjonowania polityki bezpieczeństwa cybernetycznego państw regionu Europy Środkowej.

Drugą ważną metodą użytą w pracy jest analiza systemowa, która umożliwiła potraktowanie polityki cyberbezpieczeństwa jako całości zjawiska, na które składają się poszczególne uwarunkowania i elementy wspólnie tworzące funkcjonujący system.

Uzupełnieniem obrazu podejmowanych inicjatyw przez państwa w warunkach dynamicznie zachodzących zmian w cyberprzestrzeni jest w niniejszym opracowaniu analiza instytucjonalno-prawna. Normy Unii Europejskiej odnoszące się do funkcjonowania instytucji i służb odpowiedzialnych za utrzymanie i stabilny rozwój cyberprzestrzeni stanowią ważny element w polityce europejskiej oraz są punktem odniesienia dla ośrodków władzy i podmiotów funkcjonujących w obszarze cyberbezpieczeństwa na poziomie państw V4. Zastosowanie tej analizy pozwala także na scharakteryzowanie nowych celów i zadań, które wyznaczyły przed sobą państwa V4 w 2004 roku w Deklaracji z Kromieryża, jak również w oficjalnych dokumentach i raportach mających charakter sprawozdawczy z okresu sprawowania prezydencji w Grupie Wyszehradzkiej. Istotne znaczenie w tym kontekście ma także analiza roli Międzynarodowego Funduszu Wyszehradzkiego czy też Wyszehradzkiej Grupy Bojowej UE.

Pisząc o badaniu polityki bezpieczeństwa cybernetycznego, należy wymienić metodę jakościową, która była pomocna przy analizie informacji dotyczących strategii bezpieczeństwa cybernetycznego czy też w trakcie prowadzonych badań w zakresie analizy treści oficjalnych komunikatów politycznych.

Kolejną ważną metodą badawczą, zastosowaną szczególnie w celu pozyskania danych o nieoficjalnym charakterze, był bezpośredni i indywidualny wywiad z pracownikami instytucji

zajmujących się cyberbezpieczeństwem, który miał naturę nieustandaryzowanej rozmowy, jednak z założonym z góry celem pozyskania określonych informacji w zakresie finansowania państwa oraz skali występowania cyberataków motywowanych czynnikami politycznymi.

Nie sposób pominąć w wielu miejscach pracy metody historycznej, która zastosowana została szczególnie w tych fragmentach monografii, które dotyczą początków współpracy wyszehradzkiej, a także specyficznych uwarunkowań w Europie Środkowo-Wschodniej, mających wpływ na współpracę państw V4 z Unią Europejską oraz kształtujących rozwój gospodarki cyfrowej w tym regionie Europy.

Struktura pracy odpowiada przyjętym powyżej założeniom i liczy pięć rozdziałów. Pierwszy z nich składa się z dwóch części, które dotyczą polityki bezpieczeństwa cybernetycznego UE i NATO. Rozdział ten koncentruje się przede wszystkim na działaniach instytucjonalno-prawnych, których podstawowym celem jest włączenie bezpieczeństwa cybernetycznego do głównego nurtu politycznego tych organizacji. Analiza wskazuje na etapy ewolucji cyberbezpieczeństwa, które weryfikują elastyczność oraz sprawność instytucjonalną obu organizacji wobec nowych wyzwań, jakimi są cyberzagrożenia. Analiza podjętych w rozdziale problemów badawczych dotyczy więc formalnego wkładu UE i NATO w proces ewolucji polityki cyberbezpieczeństwa.

W rozdziale drugim analizowane są uwarunkowania cybernetyczne i pozacybernetyczne charakteryzujące politykę V4. W pierwszej części nakreślona zostaje geneza powstania i dotychczasowa historia Grupy Wyszehradzkiej. W tym fragmencie pracy zasygnalizowane są także główne założenia polityki zagranicznej, która odzwierciedla zachodzące procesy w regionie Europy Środkowej. Kontynuując ten temat, przeprowadzono klasyfikację polityki państw V4, biorąc pod uwagę postawę „atlantyzmu" i „kontynentalizmu".

Analiza ta stanowi punkt wyjścia dla dalszych badań w drugiej części tego rozdziału, w którym omawiane są uwarunkowania cybernetyczne państw V4. W ramach tego fragmentu pracy dokonana zostaje charakterystyka aktywności państw wyszehradzkich w kontekście celów formułowanych podczas prezydencji V4. Badanie skupia się także na wyodrębnieniu i określeniu najważniejszych inicjatyw międzynarodowych oraz publikowanych przy tej okazji dokumentów, które stanowią materiał pozwalający określić politykę cyberbezpieczeństwa państw V4. W kolejnej części rozdziału na podstawie charakterystyki poszczególnych strategii cyberbezpieczeństwa omawiane są postawy i założenia państw Grupy Wyszehradzkiej w oparciu o zastosowanie perspektywy cywilnej i militarnej. Istotnym fragmentem tej części monografii jest analiza wydatków budżetowych przeznaczanych na inwestycje w zakresie rozwoju cyberbezpieczeństwa.

Trzeci rozdział pracy dotyczy cyberincydentów, które odnotowane zostały w obszarze państw V4. Ważne dla omawianego tematu jest wyodrębnienie określonych czynników i za ich pomocą scharakteryzowanie przeprowadzonych cyberataków w ujęciu motywacji politycznych. Kontynuacją tego tematu jest również analiza zjawiska dezinformacji, która odgrywa znaczącą rolę w przestrzeni politycznej państw Europy Środkowej.

W drugiej części rozdziału starano się odnotować działania podejmowane przez państwa V4, które stanowią reakcję na cyberzagrożenia. Omówiono zmiany w takich obszarach, jak: wymiar instytucjonalny państwa, współpraca podmiotów w zakresie wymiany informacji, partnerstwo publiczno-prywatne czy też podnoszenie jakości świadczeń usług cyfrowych przez pracowników publicznych.

W czwartym rozdziale przedstawiono charakterystykę regionów europejskich, przy czym szczególną uwagę poświęcono państwom Grupy Wyszehradzkiej w kontekście rozwoju technologii informacyjno-komunikacyjnych. Porównanie uzyskanych wyników w tym obszarze pozwala wskazać, które miejsce w Europie zajmują państwa V4 pod względem rozwoju ICT i czy można je określić mianem lidera w tym zakresie. Analiza różnicy między europejskimi regionami w ramach wykorzystania innowacji technologicznych zarówno przez przedsiębiorstwa, jak i gospodarstwa domowe wskazuje na odmienny poziom rozwoju cybertechnologii, który w dużym stopniu pokrywa się z historycznymi podziałami na wschodnią i zachodnią część Europy. Ostatni fragment rozdziału koncentruje się na wybranych aspektach życia społecznego, które w znaczący sposób uległy zmianie za pośrednictwem nowych technologii.

Piąty rozdział rozpoczyna się od scharakteryzowania głównych zjawisk zachodzących w cyberprzestrzeni, które w zależności od postrzegania i woli decydentów politycznych mogą być czynnikiem destrukcyjnym bądź wzmacniającym rozwój państwa i społeczeństwa. Odnosząc się do tego zjawiska, zauważono także, iż przestrzeń wirtualna zaczyna w wielu przypadkach dominować i zastępować sferę rzeczywistą, czego przykładem jest komunikacja przedstawicieli władzy politycznej z obywatelami. Dostrzeżono także, że cyberprzestrzeń stała się swego rodzaju alternatywnym obszarem prowadzenia polityki.

Rozdział ten stara się również uzupełnić wiedzę na temat zachodzących relacji między technologią a wolnością obywatelską. W tym celu postawiono pytanie o odporność demokracji na zachodzące procesy w cyberprzestrzeni w kontekście globalnej roli, jaką odgrywają światowe mocarstwa, takie jak: Federacja Rosyjska, Chińska Republika Ludowa oraz Stany Zjednoczone. Wykorzystanie przykładu tych państw ma pomóc uzyskać odpowiedź na pytanie, czy określone zależności między cyberzagrożeniami a rozwojem ICT i

poziomem demokracji w wymiarze globalnym są analogiczne do tych zachodzących na szczeblu regionalnym. Analiza danych w przypadku państw Grupy Wyszehradzkiej wskazuje, że skala ryzyka wystąpienia szkodliwych działań cybernetycznych jest uzależniona od poziomu rozwoju demokracji oraz wolności obywatelskich. Podobna zależność zachodzi również w przypadku zaawansowanego rozwoju ICT i stopnia upowszechnienia wolności demokratycznych.

Punktem wyjścia do dalszej analizy w tym rozdziale jest stwierdzenie, że każde z państw ma indywidualną perspektywę postrzegania zagrożeń, co jest czynnikiem różnicującym politykę cyberbezpieczeństwa członków Grupy Wyszehradzkiej. Ilustracją tego są zapisy w strategiach bezpieczeństwa cybernetycznego państw V4. Na ich podstawie przedstawiono poszczególne koncepcje, które opracowane zostały nie tylko jako przeciwdziałanie cyberzagrożeniom, ale i również jako odpowiedź na pozostałe zjawiska kształtujące przestrzeń publiczną.

W dalszej części rozdziału dokonana zostaje analiza dokumentów strategicznych, dzięki której możliwe staje się udzielenie odpowiedzi na pytanie, jak postrzegane jest samo pojęcie bezpieczeństwa cybernetycznego przez poszczególne państwa Grupy Wyszehradzkiej? Zidentyfikowane podobieństwa, jak i różnice w sposobie postrzegania rozwiązań wobec określonych problemów wskazują także na odmienne ambicje polityczne i ograniczenia w stosunku do współczesnych wyzwań stojących przed państwami V4. Ważnym jednak zapisem w każdym dokumencie strategicznym jest fragment dotyczący roli UE i NATO jako organizacji, dzięki którym realizowane są zdolności obronne państw Grupy Wyszehradzkiej.

Analiza przeprowadzona na podstawie przyjętych założeń badawczych pozwoliła na wyciągnięcie wielu wniosków oraz na weryfikację postawionych hipotez badawczych. Można zatem stwierdzić, że polityka bezpieczeństwa cybernetycznego państw V4 charakteryzuje się wysokim stopniem złożoności. Biorąc pod uwagę kierunek jej ewolucji, powstałe wnioski nie są tak jednoznaczne w interpretacji. Z jednej bowiem strony w wymiarze deklaracji politycznych oraz formułowanych celów i zadań na płaszczyźnie dokumentów strategicznych panuje ogólna zgodność co do wyznaczonych priorytetów politycznych pomiędzy państwami V4, natomiast z drugiej strony – dostrzegalne są różnice w wymiarze praktycznym, które sprowadzają się w dużej mierze do odmiennego rozłożenia akcentów w zakresie wydatków budżetowych na cyberbezpieczeństwo.

Ponadto ważnym czynnikiem mającym wpływ na spójność w ramach polityki cyberbezpieczeństwa jest różnorodność w postrzeganiu zagrożeń. Przykładem tego jest odmienny stosunek do polityki Rosji, co prowadzi do rozbieżności interesów pomiędzy

państwami wyszehradzkimi i ma również wpływ na prowadzenie działań w obszarze polityki cyberbezpieczeństwa.

Zidentyfikowane w pracy podziały polityczne wśród państw V4 przebiegają również wzdłuż podziału na „atlantyzm" utożsamiany z militarną koncepcją NATO i „kontynentalizm" odnoszący się do cyberbezpieczeństwa przede wszystkim w aspektach gospodarczym i społecznym UE. Ilustracją tego jest – wspomniany wcześniej – odmienny rozkład środków finansowych przeznaczanych na cyberobronę.

Jednocześnie podkreślić należy znaczenie rozwoju gospodarki cyfrowej oraz procesów zachodzących w wymiarze społecznym i kulturowym, które to jako całość polityki bezpieczeństwa cybernetycznego przekładają się na międzynarodową pozycję i znaczenie państwa. Wyniki badań potwierdzają istnienie podziału na wschodnią i zachodnią część Europy. Zidentyfikowane różnice korespondują zarówno z doświadczeniem historycznym państw europejskich, jak i z rzeczywistością powstałą po 1989 roku, kiedy to państwa Europy Środkowo-Wschodniej przechodziły transformację w wymiarze politycznym, gospodarczym i społecznym. Gospodarka cyfrowa państw Grupy Wyszehradzkiej w znacznym stopniu opiera się na mechanizmie produkcyjnym i odtwórczym, o czym świadczy m.in. niewielka liczba wniosków patentowych w zakresie ICT.

Na podstawie przedstawionych w pracy analiz nasuwa się wniosek, że podejmowane przez państwa V4 wysiłki na rzecz zwiększenia cyberbezpieczeństwa wymagają intensywniejszej koordynacji. W większości przypadków rządy państw Grupy Wyszehradzkiej nie są w stanie ustalić wspólnych potrzeb w zakresie infrastruktury cybernetycznej. Tak zaistniała sytuacja prowadzi do wniosku, że cyberbezpieczeństwo nie polega wyłącznie na rozwiązaniach technologicznych. Okazuje się ono kluczowym elementem w zakresie państwa i dlatego też przy analizie tego zjawiska nie można pominąć procesów politycznych, kulturowych i organizacyjnych.

Przedstawiona monografia poszerza wiedzę w zakresie dotychczasowych badań na temat polityki bezpieczeństwa państw Grupy Wyszehradzkiej, przede wszystkim ze względu na:

- zidentyfikowanie czynników pozwalających na scharakteryzowanie cyberzagrożeń w perspektywie politycznej;
- uzupełnienie wiedzy w zakresie modelu prowadzenia polityki cyberbezpieczeństwa według podziału na charakter cywilny i militarny, który koresponduje z istniejącym i analizowanym już w literaturze przedmiotu podziałem na „atlantyzm" i „kontynentalizm";

- wykorzystanie oficjalnych danych istniejących w powszechnym obiegu informacyjnym (w postaci dokumentów strategicznych czy też programów prezydencji państw V4) oraz informacji o charakterze poufnym;
- ukazanie i zbadanie czynników mających wpływ na pozycję i znaczenie państw V4 w UE, co daje również możliwość dokonania oceny rozwoju gospodarki cyfrowej w poszczególnych państwach UE;
- zestawienie procesów wewnętrznych i zewnętrznych determinujących politykę cyberbezpieczeństwa, co pozwala wskazać, które elementy mają silniejszy wpływ na poziom bezpieczeństwa państw Grupy Wyszehradzkiej;
- zwrócenie uwagi na znaczenie wymiaru społecznego w funkcjonowaniu polityki cyberbezpieczeństwa.

5. Omówienie pozostałych osiągnięć naukowo-badawczych

Pozostałe osiągnięcia naukowe uległy na przestrzeni lat ewolucji, w wyniku której dorobek naukowy można podzielić na trzy główne obszary:

a) polityka bezpieczeństwa,

b) rywalizacja polityczna,

c) sztuka i polityka.

Dokonania badawcze składają się z prac o charakterze teoretycznym oraz empirycznym, których wyniki opublikowane zostały w pięciu (łącznie z pracą habilitacyjną) monografiach autorskich, szesnastu pracach zbiorowych oraz w liczących się czasopismach naukowych. Wyniki badań prezentowane były także na konferencjach i seminariach naukowych o zasięgu ogólnopolskim, jak i międzynarodowym, w tym również poza granicami Polski. Liczba cytowań moich publikacji według programu *Publish or Perish* wynosi 17, zaś Indeks Hirsha liczony w okresie ostatnich pięciu lat wynosi 2 (15.04.2019). Oprócz tego dziewięć publikacji naukowych znajduje się na liście European Reference Index for the Humanities (ERIH) oraz jedna w bazie Journal Citation Reports (JCR).

Pierwszy obszar badań koncentruje się na zagadnieniach polityki bezpieczeństwa i składa się z 38 artykułów (w tym sześciu zagranicznych). Prace te skupiają się przede wszystkim na poszukiwaniu odpowiedzi na pytanie o rolę państwa i jego instytucji wobec współczesnych zagrożeń. W ramach omawianego tematu przedstawiona została również perspektywa

funkcjonowania demokracji w warunkach coraz bardziej powszechnych zagrożeń. Problematyce tej poświęcony jest artykuł pt. *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku*[1].

Publikacja ta omawia zagadnienia związane z funkcjonowaniem ustawy antyterrorystycznej z 2016 roku, której analiza stanowi okazję do wyznaczenia granicy pomiędzy prawem obywateli do wolności a prawem do poczucia bezpieczeństwa. Celem badań jest próba opisu najbardziej kontrowersyjnych przepisów prawnych, które ujawniają rozbieżności między dwiema wartościami, takimi jak wolność i bezpieczeństwo. W artykule opisane są także wątpliwości, które zrodziły się przy okazji obowiązywania ustawy *Patriot Act* w Stanach Zjednoczonych, a które w niektórych przypadkach są analogiczne do polskiej ustawy antyterrorystycznej. Temat artykułu bezpośrednio związany jest z próbą odpowiedzi na pytanie, czy możliwa jest do osiągnięcia równowaga pomiędzy wolnością a bezpieczeństwem?

Z powodu niesłabnącego zagrożenia atakami terrorystycznymi większość państw europejskich umieszcza ten problem na czele swoich priorytetów polityki bezpieczeństwa. Próby przeciwdziałania zagrożeniom prowokują do pojawiania się coraz to liczniejszych propozycji politycznych, z których wiele wywołuje spory i emocje społeczne. W celu przedstawienia i uporządkowania toczącej się debaty na temat znaczenia bezpieczeństwa i swobód obywatelskich zanalizowano przypadek polskiej polityki bezpieczeństwa w artykule pt. *Moral and Legal Dilemmas of the New Polish Security Policy*[2]. Punktem wyjścia do rozważań, również i w tym artykule, jest ustawa z 10 czerwca 2016 roku o działaniach antyterrorystycznych, która stała się przyczyną zbadania skomplikowanego wymiaru realizacji podstawowych zadań państwa względem swoich obywateli. Poprzez zidentyfikowanie i analizę zapisów zawartych w ustawie, na mocy których państwo może ograniczać wolności obywatelskie, możliwe stało się sformułowanie wniosku na temat ewentualnego kierunku rozwoju polityki bezpieczeństwa. Podkreślono również, że współczesnym wyzwaniem dla wielu rządów nie jest samo zapobieganie atakom terrorystycznym, ale raczej tworzenie regulacji i zapisów, w ramach których polityka antyterrorystyczna nie będzie stanowić większego zagrożenia dla demokracji niż samo zjawisko terroryzmu. Powyższe rozważania doprowadziły także do zdefiniowania kolejnego

[1] M. Górka, *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku*, „e-Politikon", 2016, nr 19, s. 47–79.

[2] M. Górka, *Moral and Legal Dilemmas of the New Polish Security Policy*, „European Review", 2019, vol. 2, s. 260-274.

dylematu, przed którym stoją państwa demokratyczne. Rozstrzygnąć bowiem należy, na ile współczesna polityka bezpieczeństwa oraz przepisy prawne powinny zapewnić udogodnienia dla funkcjonowania i realizacji zadań przez służby odpowiedzialne za bezpieczeństwo, a na ile powinny gwarantować kontrolę nad nimi.

Kolejnym artykułem dotyczącym związków między polityką a bezpieczeństwem jest współautorska praca pt. *Public sentiment after the terrorist attacks and their impact on the attitudes on Polish people*[3]. W publikacji omawiane są współczesne zagrożenia w postaci terroryzmu i ich wpływu na postawy społeczne, jak i na decyzje polityczne rządów państw europejskich. Artykuł stanowi próbę odpowiedzi na pytanie, czy wzrost zagrożenia terrorystycznego pociąga za sobą zwiększone poparcie dla ruchów radykalnych, populistycznych i nacjonalistycznych. Ważnym polem badań, obrazującym postawy społeczne wobec zagrożeń, jest analiza społeczeństwa w perspektywie podziałów socjodemograficznych, które przebiegają wzdłuż podziałów ideologicznych.

Problematyka dotycząca funkcjonowania państwa w obliczu narastających zagrożeń kontynuowana jest w artykule pt. *Polityka antyterrorystyczna jako dylemat demokracji liberalnej*[4]. Podjęta w pracy analiza stanowi próbę opisu wzajemnych relacji pomiędzy zjawiskiem terroryzmu a demokracją liberalną. Jak można zauważyć, oba zjawiska nie tylko silnie oddziaływują na siebie, ale również kształtują sposób funkcjonowania państwa oraz jego obywateli. Podkreślono także, iż poza widocznymi i bezpośrednimi skutkami ataków na osoby postronne, zamachy terrorystyczne osłabiają wartości demokratyczne, w tym również zaufanie do instytucji państwowych i praw regulujących ich funkcjonowanie. Zawarty w artykule wniosek wskazuje, że jednym z podstawowych i niezmiennych wciąż problemów liberalnej demokracji jest zmaganie się z napięciem powstałym między dwiema wartościami, czyli wolnością i bezpieczeństwem, co stanowi punkt wyjścia do dalszych analiz badawczych.

Na kanwie rozważań na temat praw i wolności obywatelskich wobec współczesnych zagrożeń poruszona zostaje również kwestia wyzwań, jakie nowe technologie stwarzają wobec państwa. Powstaje zatem pytanie: jaką politykę bezpieczeństwa powinny prowadzić rządy, aby zapewnić stabilny rozwój państwa i jego obywateli oraz gwarantować wolność, a jednocześnie odpowiadać na szybko zachodzące zmiany technologiczne?

---

[3]M. Górka, U. Soler, *Public sentiment after the terrorist attacks and their impact on the attitudes on Polish people,* „Security, Terrorism and Society", 2017, nr 5, s. 89–110.

[4]M. Górka, *Polityka antyterrorystyczna jako dylemat demokracji liberalnej*, „Świat Idei i Polityki", 2017, nr 4, s. 122–137.

Aby odpowiedzieć na to pytanie, w artykule pt. *Kultura bezpieczeństwa w kontekście znaczenia informacji jako elementu społeczno-kulturowego* [5], postanowiono rozpocząć omówienie tego problemu od analizy związku między kulturą polityczną a kulturą bezpieczeństwa. Celem publikacji jest także opis znaczenia bezpieczeństwa cybernetycznego, którego definicja odnosi się nie tylko do wymiaru technologii, ale i określonych idei, norm oraz zasad, które kształtują egzystencję współczesnego człowieka i pozwalają mu funkcjonować w rzeczywistości wirtualnej. Na podstawie zidentyfikowanych w przestrzeni publicznej procesów oraz literatury przedmiotu dokonana zostaje w pracy próba stworzenia pojęcia kultury cyberbezpieczeństwa. Istotne również dla poruszanego tematu staje się skoncentrowanie uwagi na edukacji, która stanowi między innymi narzędzie promocji określonych zasad i wartości. Zaznaczyć jednak należy, że sfera kultury, zarówno w zakresie polityki, jak i bezpieczeństwa, jest niezwykle skomplikowanym i wielowymiarowym procesem, w którym oba te obszary wzajemnie się przenikają. A zatem bez zrozumienia znaczenia kultury nie sposób jest skutecznie rozwiązać współczesnych wyzwań w wymiarze cyberbezpieczeństwa. Każde bowiem państwo ma swoją własną kulturę polityczną, a także kulturę bezpieczeństwa cybernetycznego, co oznacza, że istnieje różny stopień wrażliwości na konkretne incydenty oraz wydarzenia zarówno w świecie rzeczywistym, jak i wirtualnym.

Wyrazem kontynuacji zainteresowań badawczych w zakresie polityki bezpieczeństwa cybernetycznego jest artykuł: *Cybersecurity as a challenge for modern state and society*[6]. Publikacja ma na celu omówienie praktyk związanych z operacjami sieciowymi prowadzonymi przez państwa i podmioty niepaństwowe. Opisuje także charakter i dynamikę konfliktów w cyberprzestrzeni, które przynoszą negatywne konsekwencje dla państwa i społeczeństwa, jednak charakterystyka dotychczasowych działań realizowanych przez państwo wskazuje, że cyberzagrożenia stanowią także impuls do pozytywnych zmian w zakresie polityki cyberbezpieczeństwa. W trakcie analizy tematu odnotowano, że obecna przestrzeń publiczna, która oparta jest w dużym stopniu na cybertechnologii, redefiniuje dotychczasowy model współpracy i rywalizacji pomiędzy różnymi podmiotami zarówno na poziomie lokalnym, jak i międzynarodowym. W pracy podjęto również próbę zanalizowania wybranych wątpliwości pojawiających się często w literaturze przedmiotu, które dotyczą szczególnie wartościowania i kategoryzowania cyberzagrożeń.

---

[5] M. Górka, *Kultura bezpieczeństwa w kontekście znaczenia informacji jako elementu społeczno-kulturowego*, „Przegląd Politologiczny", 2018, nr 2, s. 105–121.

[6] M. Górka, *Cybersecurity as a challenge for modern state and society*, „Acta Politica Polonica", 2018, nr 2, s. 29–39.

W obszar badań nad polityką bezpieczeństwa cybernetycznego wpisuje się również artykuł pt. *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*[7]. Publikacja ta jest efektem prowadzonych konsultacji naukowych w ramach uczestnictwa w Polskim Towarzystwie Oceny Technologii. Praca wskazuje na procesy technologiczne, które aktywnie towarzyszą oraz determinują funkcjonowanie otoczenia społeczno-politycznego. Ponadto podkreślona zostaje rola nauk społecznych, bez których trudno jest obecnie wyjaśnić i rozwiązać problemy związane z technologią informacyjno-komunikacyjną i jej zastosowaniem. Na tej podstawie analiza podjętego tematu wskazuje na szeroki zakres stosowania technologii w przestrzeni publicznej, czego ilustracją są m.in. narzędzia cyfrowe regulujące codzienne życie. Prowadzi to do stanu symbiozy, w której trudno jest wskazać przewagę technologii bądź społeczeństwa w tak zaistniałej rzeczywistości.

Jednocześnie w ramach omawianego problemu polityki cyberbezpieczeństwa uwaga skupiona została na zagadnieniach związanych z uwarunkowaniami obronnymi państwa. Artykuł pt. *Cyberconflicts as a Threat for the Modern State*[8] podkreśla obecność wielu procesów zachodzących w przestrzeni międzynarodowej, które nabywają nowego charakteru zwłaszcza w wyniku rewolucji cyfrowej. W trakcie analizy tematu zauważono także, iż zagrożenia o charakterze ponadnarodowym bardzo często determinują politykę wewnętrzną państwa. Publikacja omawia zagadnienia związane z funkcjonowaniem cyberprzestrzeni, która stała się czynnikiem determinującym strategiczne i ekonomiczne koncepcje państwa. Artykuł zwraca uwagę na postępujący wzrost znaczenia cyberprzestrzeni, czego przykładem jest strategia wielu rządów, które w swych planach i założeniach politycznych biorą pod uwagę prowadzenie operacji obronnych i ofensywnych z wykorzystaniem nowych technologii.

W obszar badań nad polityką cyberbezpieczeństwa wpisują się również dwa kolejne artykuły poświęcone przede wszystkim regionalnemu wymiarowi tego zjawiska. Pierwszy z nich dotyczy inicjatywy politycznej skupionej wokół dwunastu państw, które tworzą wspólnie koncepcję Trójmorza. W artykule pt. *The Three Seas Initiative as a political challenge for the countries of Central and Eastern Europe*[9] scharakteryzowano uwarunkowania polityczne oraz gospodarcze państw Europy Środkowo-Wschodniej, które w znaczny sposób wpływają na odmienne definiowanie interesów narodowych przez poszczególne rządy tego regionu.

---

[7] M. Górka, *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Zeszyty Naukowe Politechniki Śląskiej", 2017, nr 5, s. 73–89.

[8] M. Górka, *Cyberconflicts as a Threat for the Modern State,* „Computer Science and Information Technology", 2017, vol. 6/6, s. 11–20.

[9] M. Górka, *The Three Seas Initiative as a political challenge for the countries of Central and Eastern Europe*, „Politics in Central Europe", 2018, nr 2, s. 55–73.

Zakładając, że postępujący rozwój technologii informacyjno-komunikacyjnych w coraz większym stopniu zaczyna odgrywać rolę w polityce międzynarodowej, w artykule postanowiono zanalizować możliwości tworzenia regionalnej polityki cyberbezpieczeństwa opartej m.in. na projektach budowy wspólnych sieci teleinformatycznych. Tego typu przedsięwzięcia z pewnością wzmacniają potencjał gospodarczy oraz bezpieczeństwo cybernetyczne tego regionu, co często również podkreślane jest w oficjalnych postulatach przez rządy państw Trójmorza. W pracy zbadano także – na podstawie wybranych wskaźników gospodarczych oraz społecznych – potencjał cybernetyczny Europy Środkowo-Wschodniej, który porównany został do poziomu rozwoju wszystkich państw UE, a także do takich państw, jak: Stany Zjednoczone, Federacja Rosyjska oraz Chińska Republika Ludowa. W tym kontekście przeprowadzona analiza wskazuje na niekorzystny poziom rozwoju gospodarki cyfrowej wśród poszczególnych członków Inicjatywy Trójmorza. W pracy podkreślono także rozbieżności w postrzeganiu i prowadzeniu polityki cyberbezpieczeństwa przez poszczególne państwa.

Drugim wspomnianym artykułem, będącym kontynuacją omawianych zjawisk zachodzących w regionie państw Europy Środkowej, jest praca pt. *Cybersecurity strategy of the Visegrad Group countries*[10]. Publikacja koncentruje się na polityce bezpieczeństwa cybernetycznego państw Grupy Wyszehradzkiej i ma na celu, opierając się na analizie dokumentów strategicznych, wskazanie podobieństw oraz różnic między tymi państwami w postrzeganiu cyberzagrożeń. Wnioski powstałe na podstawie przeprowadzonych badań mają istotne znaczenie dla określenia i dokonania oceny w stosunku do przyszłej współpracy w zakresie wspólnej strategii bezpieczeństwa cybernetycznego w regionie Europy Środkowej. Ponadto artykuł wskazuje, że strategie bezpieczeństwa cybernetycznego są dokumentami sformułowanymi przez określone środowiska polityczne i w określonym kontekście politycznym, przez co znajdujące się w nich zapisy odzwierciedlają interesy i priorytety określonych rządów, to z kolei pozwala na szersze scharakteryzowanie polityki wybranego państwa. Przeprowadzone badanie stanowi także okazję do postawienia hipotez na temat przyszłej współpracy państw Grupy Wyszehradzkiej w obszarze cyberbezpieczeństwa.

Zagadnienia badawcze zasygnalizowane w powyższym artykule znajdują również kontynuację w pracy pt. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej w*

[10]M. Górka, *Cybersecurity strategy of the Visegrad Group countries,* „Politics in Central Europe", 2018, vol. 14/2, s. 75–98.

kontekście zagrożeń dla egzystencji państwa w XXI wieku[11]. Celem artykułu jest zbadanie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, dzięki czemu możliwe staje się scharakteryzowanie, po pierwsze: sposobu w jaki decydenci polityczni postrzegają poziom cyberbezpieczeństwa; po drugie: które z obszarów państwa stanowią newralgiczne elementy jego bezpieczeństwa. Dokumenty strategiczne pozwalają więc usystematyzować przez państwo obraz własnego potencjału cybernetycznego wraz z możliwymi zagrożeniami. Ponadto określają podstawowe priorytety dla cyberegzystencji państwa oraz wskazują na główne zadania instytucji publicznych w ramach polityki cyberbezpieczeństwa.

Uzyskane wyniki wskazują, że państwo koncentruje się na kilku aspektach; z jednej strony uwaga decydentów politycznych skupia się na ekonomicznym wpływie cyberprzestępczości i walce z tym zjawiskiem, z drugiej – akcentowane są również czynniki militarne. Jednak dominującym elementem w cyberstrategii są fragmenty poświęcone cyberzagrożeniom skierowanym na infrastrukturę krytyczną państwa.

Pozostałe artykuły w dorobku naukowym, wchodzące w obszar badań polityki bezpieczeństwa, jak m.in.: *Czynniki społeczno-kulturowe a bezpieczeństwo publiczne w UE*[12] oraz *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*[13], korespondują z wnioskami badawczymi w powyższych pracach.

W realizowanych badaniach nad polityką bezpieczeństwa uwaga badawcza skupiona była także na funkcjonowaniu wywiadu i kontrwywiadu oraz ich istotnemu znaczeniu dla procesów decyzyjnych w środowiskach politycznych wielu państw. Zagadnieniu temu poświęconych zostało dziewięć artykułów naukowych oraz dwie prace zbiorowe: *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa*[14] oraz *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku* [15]. Efektem badań nad funkcjonowaniem wywiadu jest także monografia pt. *Mossad. Porażki i sukcesy tajnych służb*

---

[11] M. Górka, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej w kontekście zagrożeń dla egzystencji państwa w XXI wieku,* [w:] *Partie i ugrupowania polityczne wobec polityki bezpieczeństwa Polski w XXI wieku. Założenia i realizacja wybranych programów politycznych*, red. M. Kamola-Cieślik, Ł. Tomczak, Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego 2017, s. 179–191.

[12] M. Górka, *Czynniki społeczno-kulturowe a bezpieczeństwo publiczne w UE*, [w:] *Społeczne i kulturowe wymiary bezpieczeństwa*, red. Z. Danielewicz, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2013, s. 73–84.

[13] M. Górka, *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*, „Przegląd Geopolityczny", 2018, nr 25, s. 86–103.

[14] *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa*, red. M. Górka, Adam Marszałek, Toruń: Wydawnictwo Adam Marszałek 2016.

[15] *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, red. M. Górka, Warszawa: Wydawnictwo Difin 2016.

izraelskich[16]. Państwo Izrael stanowi tu punkt wyjścia do analizy służb, które w przypadku pozostałych państw działają w skomplikowanym otoczeniu wielu wzajemnie krzyżujących się procesów społecznych, politycznych i technologicznych. Dlatego w pracy starano się zanalizować nowe wyzwania, przed którymi stoi współczesne państwo oraz społeczność wywiadowcza. Monografia jest także próbą ilustracji zachodzących zjawisk, które mają wpływ na ewolucję polityki bezpieczeństwa.

Okazuje się zatem, że analiza tematu służb wywiadowczych stanowi ważne uzupełnienie stanu wiedzy w zakresie nauk o polityce, bowiem każde państwo dąży do osiągnięcia bezpieczeństwa w długoterminowej perspektywie, a odbywa się to m.in. na podstawie danych wywiadowczych. Wywiad analizuje również możliwe scenariusze rozwoju sytuacji pod kątem ich wiarygodności oraz ewentualnych konsekwencji dla funkcjonowania państwa. Zrozumienie wielu uwarunkowań kształtujących politykę międzynarodową potraktować można jako jeden z głównych obszarów pracy służb. Zagadnieniu temu poświęcony został artykuł pt. *Dyplomacja i wywiad. Przyczynek do refleksji nad polityką bezpieczeństwa*[17].

W publikacjach na temat pracy wywiadu uwzględnione zostają również zmiany wynikające z czynników zewnętrznych na arenie międzynarodowej, takie jak m.in. postęp technologiczny, czego wyrazem jest m.in. praca pt. *Wybrane problemy z teorii wywiadu cybernetycznego*[18].

Podstawowym obszarem wywiadu jest analiza źródeł informacji, która pozwala zrozumieć decyzje rządu oraz działania służb obcego państwa. Dla większości reżimów skuteczność wywiadu stanowi nie tylko gwarancję bezpieczeństwa, lecz także możliwość zdobycia oraz zachowania przewagi politycznej i gospodarczej w wysoko konkurencyjnym środowisku międzynarodowym. W ten nurt wpisują się dwie pozostałe publikacje pt. *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*[19] oraz *Otwarte źródła informacji – nowa czy klasyczna formuła wywiadu?*[20].

---

[16] M. Górka, *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa: Wydawnictwo Difin 2015.

[17] M. Górka, *Dyplomacja i wywiad. Przyczynek do refleksji nad polityką bezpieczeństwa*, [w:] *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, red. M. Górka, Warszawa: Wydawnictwo Difin 2016, s.64-82.

[18] M. Górka, *Wybrane problemy z teorii wywiadu cybernetycznego*, „Kwartalnik Bellona", 2017, nr 3, s. 49–62.

[19] M. Górka, *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*, „Środkowoeuropejskie Studia Polityczne", 2017, nr 2, s. 105–125.

[20] M. Górka, *Otwarte źródła informacji – nowa czy klasyczna formuła wywiadu?*, [w:] *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa*, red. M. Górka, Toruń: Wydawnictwo Adam Marszałek 2016, s. 19–47.

Ważnym obszarem analiz w tym nurcie badawczym są także prace pt. *Rola ABW w polskiej polityce bezpieczeństwa*[21] oraz *Wybrane elementy bezpieczeństwa narodowego w perspektywie wywiadu i kontrwywiadu w sektorze gospodarczym*[22]. Opracowania te podkreślają uwarunkowania polityczno-gospodarcze, które stanowią ważny obszar pracy wywiadu. Wyniki analizy zwracają również uwagę na zadania służb w zakresie ochrony informacji, które stanowią współcześnie – w warunkach cyberzagrożeń – ważny element rozwoju gospodarki państwa.

Zainteresowania naukowe, obok polityki bezpieczeństwa, obejmują także zagadnienia związane z perspektywą społeczną i skupiają się na eksplorowaniu obszarów, które w niewystarczającym stopniu podejmowane były wcześniej w literaturze z dziedziny nauk społecznych. Proces ewolucji postaw obywateli polegający m.in. na zmianie ich zachowań, który następuje w wyniku upowszechnienia cybertechnologii, jest szczególnie interesujący poznawczo dla nauk o polityce. Przejawem tego jest mowa nienawiści, która coraz częściej dominuje w dyskursie publicznym. Tematowi temu poświęcony jest artykuł pt. *Education of young people and children as a way of fighting against Internet hate, a form of cyber violence*[23]. Podjęta w pracy analiza cyberagresji słownej podkreśla potrzebę inicjowania działań związanych z edukacją obywatelską. Kontynuacją tych badań jest kolejny artykuł pt. *Kłamstwa na czatach. Wirtualne zagrożenia a realny problem*[24], który wskazuje, że popełniane dotychczas przestępstwa coraz częściej mają swój odpowiednik w wirtualnej przestrzeni.

Powszechnie dostępne urządzenia mobilne oraz za ich pomocą aplikacje i serwisy społecznościowe poprawiają standard życia wielu osób. Jednak to, co może tworzyć innowacyjność w codziennym życiu, może stanowić także ogromne zagrożenie, z którego nie każda osoba zdaje sobie sprawę. Problematyce tej poświęcona została praca pt. *Od ekshibicjonizmu po teatralizację, czyli o zagrożeniach wynikających z cyberuzależnienia*[25]. Publikacja porusza kwestię upubliczniania informacji, w tym również o charakterze

---

[21] M. Górka, *Rola ABW w polskiej polityce bezpieczeństwa*, [w:] *Współczesne wymiary polskiej polityki bezpieczeństwa*, red. M. Górka, Warszawa: Wydawnictwo Difin 2014, s. 176–190.

[22] M. Górka, *Wybrane elementy bezpieczeństwa narodowego w perspektywie wywiadu i kontrwywiadu w sektorze gospodarczym*, [w:] *Służby mundurowe w systemie bezpieczeństwa publicznego*, red. M. Kopczewski, D. Sienkiewicz, Koszalin: Wydawnictwo Centrum Szkolenia sił Powietrznych w Koszalinie 2016, s.99-116.

[23] M. Górka, *Education of young people and children as a way of fighting against Internet hate, a form of cyber violence*, „Journal of Educational Sciences", 2017, nr 2/36, s. 26–41.

[24] M. Górka, *Kłamstwa na czatach. Wirtualne zagrożenia a realny problem*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa: Wydawnictwo Difin 2014, s. 148–159.

[25] M. Górka, *Od ekshibicjonizmu po teatralizację, czyli o zagrożeniach wynikających z cyberuzależnienia*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny czy wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa: Wydawnictwo Difin 2017, s. 88–105.

prywatnym, które z jednej strony mogą stanowić zagrożenia dla konkretnych użytkowników, ale z drugiej są często przejawem kreowania wizerunku publicznego, który stał się również popularnym zjawiskiem promocji we współczesnej polityce.

Sfera obyczajowa, która uległa w ostatnim czasie znaczącej zmianie pod wpływem m.in. cyberprzestrzeni, ma również wpływ na systemem wartości panujący w społeczeństwie. Przykładem tego jest m.in. stosunek do takich problemów, jak: aborcja, eutanazja, postrzeganie mniejszości seksualnych itp. W tym znaczeniu interesująca wydaje się analiza sfery obyczajowej. Jej przykładem jest zjawisko prostytucji, której problem zaliczany jest do sfery polityki społecznej państwa. Wątek ten poruszony został w artykule pt. *Prostytucja i cyberprostytucja jako specyficzne zagrożenie dla młodych ludzi*[26].

W kontekście wielu istniejących cyberzagrożeń pojawiła się potrzeba zastosowania szerokich, obejmujących wiele instytucji oraz grup społecznych, działań edukacyjnych. Wyrazem tego było zainicjowanie współpracy pomiędzy wybranymi instytucjami na szczeblu samorządowym w okresie 2013–2015. Wyniki badań przeprowadzone w ramach realizowanego programu zostały opublikowane w artykule pt. *Projekt modelu grupy dyspozycyjnej jako innowacyjnej współpracy w zakresie cyberbezpieczeństwa wśród dzieci i młodzieży*[27]. Celem analizy była weryfikacja zależności między działaniami edukacyjnymi w zakresie cyberbezpieczeństwa a skalą występowania zagrożeń wśród wybranej grupy dzieci i młodzieży. Publikacja omawia model współpracy w zakresie cyberbezpieczeństwa, który jednocześnie może być realizowany w innych obszarach rozwoju lokalnego.

Drugi z wymienionych nurtów badawczych koncentruje się na procesie rywalizacji politycznej. W tym obszarze opublikowano 21 artykułów naukowych oraz dwie monografie autorskie.

Podsumowaniem wieloletnich zainteresowań badawczych polską sceną polityczną jest monografia pt. *PO-PiS-owa demokracja. Rywalizacja partyjna w latach 2005–2015*[28]. Stanowi ona kompleksową analizę najważniejszych zjawisk mających miejsce na polskiej scenie politycznej w okresie 2005–2015. Szeroko omówione zostało w niej zjawisko

---

[26]M. Górka, *Prostytucja i cyberprostytucja jako zagrożenie dla młodych ludzi*, „Studia Edukacyjne", 2017, nr 46, s. 307–324.

[27] M. Górka, *Projekt modelu grupy dyspozycyjnej jako innowacyjnej współpracy w zakresie cyberbezpieczeństwa wśród dzieci i młodzieży*, [w:] *Zadania jednostek administracyjnych samorządu terytorialnego z wykorzystaniem potencjału grup dyspozycyjnych w przezwyciężaniu zagrożeń bezpieczeństwa publicznego*, red. J. Maciejewski, M. Stochmal, A. Sokołowska, Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego 2016, s. 129-146.

[28]M. Górka, *PO-PiS-owa demokracja. Rywalizacja partyjna w latach 2005–2015*, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2017.

rywalizacji między dwiema partiami politycznymi, czyli Prawem i Sprawiedliwością oraz Platformą Obywatelską. Rozprawa identyfikuje oraz omawia konsekwencje wynikające z dominacji na polskiej scenie politycznej tych dwóch środowisk politycznych. Książka w zamierzeniu jest także kontynuacją pracy Mirosławy Grabowskiej pt. *Podział Postkomunistyczny. Społeczne podstawy polityki w Polsce po 1989 roku*[29].

Drugą monografią wpisującą się w kontekst rywalizacji politycznej jest *Karnawał i media jako determinanty współczesnej polityki*[30]. W publikacji starano się określić w całościowy sposób funkcjonowanie współczesnej polityki w perspektywie karnawalizacji ujętej na gruncie literaturoznawstwa przez Michaiła Bachtina. Praca wskazuje, że współczesne życie polityczne jest bogate w elementy groteski, zabawy, ironii oraz profanacji, co szczególnie jest widoczne podczas kampanii wyborczych. W tym kontekście interpretacja w kategorii karnawału pozwala spojrzeć z szerszej perspektywy na zachowania wyborców i polityków, kulturę polityczną oraz funkcjonowanie środków masowego przekazu.

Interpretacja karnawalizacji może być więc kluczem do analizy relacji między władzą, wyborcami a mediami. Problematyka ta jest kontynuacją refleksji naukowych obecnych w artykułach pt. *The „meme" as an example of carnivalized internet communication*[31] oraz *Carnivalesque elements in protests of belarusian opposition*[32]. Obie prace podkreślają, że choć polityka i karnawał mogą wydawać się od siebie odległe, to jednak można w nich dostrzec pewne analogie i podobieństwa. Karnawał jest wyjątkowym i zupełnie odmiennym od codziennej rzeczywistości miejscem i czasem, analogicznym do kampanii wyborczych, które z jednej strony stanowią formę kolorowego święta, z drugiej – są zapowiedzią nadchodzących zmian społeczno-politycznych. Niektóre działania opozycji białoruskiej również skłaniają do postawienia tezy o skarnawalizowanych formach protestów politycznych, w których krytyka władzy przedstawiona w formie prześmiewczej satyry stanowi narzędzie społecznego buntu.

Jednocześnie w ramach omawianego obszaru badawczego przedstawione zostały wybrane aspekty rywalizacji politycznej, które kształtowały przebieg kampanii wyborczych. Podejmowane tematy miały na celu przybliżenie oraz wyjaśnienie zachodzących zjawisk w

---

[29] M. Grabowska, *Podział postkomunistyczny. Społeczne podstawy polityki w Polsce po 1989 roku*, Warszawa: Wydawnictwo Scholar 2004.

[30] M. Górka, *Karnawał i media jako determinanty współczesnej polityki*, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2015.

[31] M. Górka, *The „meme" as an example of carnivalized internet communication*, „e-Politikon", 2014, nr 9, s. 215–242.

[32] M. Górka, *Carnivalesque elements in protests of belarusian opposition*, The Third International Congress of Belarusian Studies, (Трэці Міжнародны Кангрэс даследчыкаў Беларус), Vytautas Magnus University Press Kaunas, Lithuania, 2014, t.3, s.161-164.

przestrzeni polskiej polityki. Przykładem tego jest artykuł pt. *Kryzys lewicy w Polsce. Casus SLD przed i po 2005 roku*[33]. Podjęto w nim próbę zdefiniowania zjawisk prowadzących do nowego modelu rywalizacji politycznej, w której dominującą rolę odgrywają partie postsolidarnościowe. Opracowanie skupia się również na badaniu procesów zachodzących w ramach elektoratu SLD, którego analiza stanowi klucz do zrozumienia słabych wyników wyborczych środowisk lewicowych w Polsce.

Kontynuacją tego tematu jest publikacja pt. *Ewolucja systemu partyjnego w województwie zachodniopomorskim w kontekście wyborów samorządowych* [34] . Celem artykułu jest wyjaśnienie wyników wyborczych partii politycznych biorących udział w kampanii samorządowej w 2014 roku w regionie województwa zachodniopomorskiego. Analiza koncentruje się szczególnie na poparciu politycznym dla Sojuszu Lewicy Demokratycznej i stara się wyjaśnić uwarunkowania dotychczasowych preferencji politycznych, które zmierzały w kierunku Platformy Obywatelskiej.

Następną pracą w ramach eksploracji problematyki rywalizacji wyborczej jest artykuł pt. *Wybory w Rosji 2011 i 2012 roku. Zmiana czy stagnacja społeczno-polityczna?*[35]. Celem tego opracowania było scharakteryzowanie zmian w zakresie sporów politycznych w Rosji, które zainicjowane zostały w wyniku odbywających się kampanii wyborczych. W analizie wyszczególniono czynniki dynamizujące rywalizację wyborczą, a także wskazano, na jakich wartościach i hasłach koncentrowała się uwaga publiczna. Analiza manifestacji towarzyszących wyborom w Rosji pozwoliła także wskazać na nowe formy protestów.

W badaniach zwrócono szczególną uwagę na czynniki związane z cybertechnologią, które w znaczny sposób kształtowały przebieg kampanii wyborczych. W ten nurt badań wpisuje się również artykuł pt. *Zjawisko cyberpopulizmu na przykładzie Twittera Donalda Trumpa podczas kampanii prezydenckiej w 2016 roku*[36]. Celem niniejszego artykułu jest także ocena roli, jaką media społecznościowe odgrywają w zakresie poparcia wyborczego względem wybranego polityka. W podjętej analizie starano się zrozumieć, w jaki sposób internet jest wykorzystywany przez polityków oraz jak przyczynia się on do manifestacji oraz rozpowszechniania populizmu. Z tego też powodu w niniejszym opracowaniu podjęta zostaje

---

[33]M. Górka, *Kryzys lewicy w Polsce. Casus SLD przed i po 2005 roku*, [w:] *Partie polityczne w Polsce i w Europie. Struktury, funkcje, strategie w zmieniającym się otoczeniu,* red. A. Pacześniak, M. Wincławska, Wrocław – Toruń 2013, s. 179–197.

[34]M. Górka, *Ewolucja systemu partyjnego w województwie zachodniopomorskim w kontekście wyborów samorządowych*, „Przegląd Zachodniopomorski", 2014, nr 1, s. 53–76.

[35]M. Górka, *Wybory w Rosji 2011 i 2012 roku. Zmiana czy stagnacja społeczno-polityczna?*, „Wrocławskie Studia Politologiczne", 2014, nr 16, s. 186–204.

[36] M. Górka, *Zjawisko cyberpopulizmu na przykładzie Twittera Donalda Trumpa podczas kampanii prezydenckiej w 2016 roku*, „e-Politikon", 2017, nr 24, s. 112–134.

próba opisu formy komunikacji na Twitterze przez kandydata na urząd prezydenta USA. Głównym wnioskiem sformułowanym w artykule jest stwierdzenie, że populizm przejawia się nie tylko w konwencjonalnych wystąpieniach publicznych, znanych do tej pory z manifestacji i debat politycznych, lecz także obecny jest w mediach społecznościowych, czego dowodem jest kampania prezydencka w USA w 2016 roku.

Kolejnym artykułem odnoszącym się do zagadnień związanych z rywalizacją polityczną w cyberprzestrzeni jest opracowanie pt. *Cybertools of political competition in the U.S. presidential campaign of 2016* [37]. Praca stanowi ocenę skuteczności wykorzystania cyberprzestrzeni w celu komunikacji politycznej kandydatów na urząd prezydenta USA z wyborcami w 2016 roku. Wiele wydarzeń, które miały miejsce podczas tych wyborów, było przełomowych nie tylko w zakresie stosowania na szeroką skalę cybernarzędzi, lecz także w perspektywie zaangażowania obcych podmiotów politycznych w wewnętrzne sprawy USA. W następstwie doniesień i spekulacji medialnych sformułowano podejrzenia, że fałszywe wiadomości mogły mieć decydujące znaczenie w wyborze Donalda Trumpa na urząd prezydenta. Zaprezentowana analiza danych z okresu kampanii wyborczej dotyczy wpływu wydarzeń politycznych na proces poparcia dla obu kandydatów i stara się wyjaśnić, które momenty miały decydujący znaczenie na zwycięstwo wyborcze. Ponadto praca wskazuje na cyberzagrożenia, które mogą kształtować przebieg rywalizacji politycznej.

Oprócz badań nad rywalizacją wyborczą istotnym problemem, który został poddany naukowej analizie, było zjawisko przywództwa politycznego. Wspólnym mianownikiem w podejmowanych tematach rozpraw jest pojęcie charyzmy.

Nie ulega wątpliwości, że funkcjonowanie grup społecznych oraz instytucji publicznych – szczególnie w szybko zmieniającym się otoczeniu – wymaga przywództwa. Istnieje także ścisły związek między zmianami w instytucji na stanowisku lidera a poziomem i jakością wykonywanych obowiązków wśród jej pracowników. Zagadnieniu temu poświęcony jest artykuł pt. *Wizerunek lokalnego przywódcy we współczesnej instytucji samorządowej* [38]. Rozważania w pracy prowadzą do wniosku, że charyzmatyczne przywództwo może być silnym bodźcem dla innowacyjności, rozwoju i gotowości do zmian. Wartością wzbogacającą treść opracowania są badania przeprowadzone wśród pracowników instytucji publicznych oraz osób piastujących kierownicze stanowiska w organizacjach znajdujących się w regionie województwa zachodniopomorskiego. Tak zestawione ze sobą dane wykazały w trakcie

[37] M. Górka, *Cybertools of political competition in the U.S. presidential campaign of 2016*, „Polish Political Science Yearbook", 2018, vol. 47/4, s. 628–642.

[38] M. Górka, *Wizerunek lokalnego przywódcy we współczesnej instytucji samorządowej*, „Przegląd Zachodniopomorski", 2013, nr 4, s. 61–82.

analizy potrzebę obecności skutecznego lidera w instytucjach, a także wskazały na ogromny dystans oraz brak zrozumienia pomiędzy dwiema badanymi grupami.

Następną pracą jest artykuł pt. *Przywództwo polityczne Jarosława Kaczyńskiego i Donalda Tuska w latach 2005–2011. Wybrane aspekty*[39]. Celem tekstu jest wskazanie oraz zrozumienie okoliczności, które wykreowały wizerunek tych polityków. Analiza prowadzi do wniosku, że przywództwo jest efektem okoliczności zewnętrznych, które tworzą osobowość przywódcy. Podjęta została także refleksja na temat roli, jaką odgrywają środki masowego przekazu w kreowaniu wizerunku publicznego. Badanie tych zjawisk jest kontynuowane w pracy pt. *Model przywództwa pseudocharyzmatycznego w wyborach parlamentarnych 2007 roku*[40] oraz w publikacji współautorskiej pt. *Partie populistyczne na przykładzie wyborów parlamentarnych w 2007 roku*[41]. Oba opracowania wskazują na zachodzące zjawisko personalizacji politycznej, polegające m.in. na postrzeganiu środowisk politycznych przez pryzmat ich lidera.

Kolejnym omówieniem w ramach opisywanego zagadnienia jest artykuł analizujący przywództwo charyzmatyczne przedstawione w perspektywie społeczno-religijnej. Charakterystyka tego zjawiska została opisana w pracy pt. *Przywództwo charyzmatyczne księdza Jerzego Popiełuszki*[42]. Celem tej publikacji jest wskazanie, że charyzma występuje na wielu płaszczyznach życia publicznego. Ponadto artykuł bada czynniki będące wynikiem otoczenia społeczno-politycznego, które kształtują postrzeganie lidera przez odbiorców.

Trzeci nurt badań koncentruje uwagę na związkach sztuki i polityki, które korespondują z zachodzącymi procesami politycznymi i stanowią ich zapis. Ważnym osiągnięciem naukowym w tym obszarze jest monografia pt. *Leopold Tyrmand – kontestator komunizmu. Rzeczywistość dekady stalinowskiej w zwierciadle Dziennika 1954 oraz prasy PRL*[43] oraz będąca kontynuacją tych analiz praca zbiorowa pt. *U brzegów Leopolda Tyrmanda*[44].

Obie publikacje stanowią istotny wkład w rozwój wiedzy na temat uwarunkowań życia codziennego w PRL. Osobista perspektywa zapisana w *Dzienniku 1954* stanowi punkt

---

[39] M. Górka, *Przywództwo polityczne Jarosława Kaczyńskiego i Donalda Tuska w latach 2005–2011. Wybrane aspekty*, „Forum Politologiczne", 2013, nr 15, s. 177–205.

[40] M. Górka, *Model przywództwa pseudocharyzmatycznego w wyborach parlamentarnych 2007 roku*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Acta Politica", 2012, nr 24, s. 121–146.

[41] M. Górka, D. Magierek, *Partie populistyczne na przykładzie wyborów parlamentarnych w 2007 roku*, „Wrocławskie Studia Politologiczne", 2012, nr 13, s. 107–123.

[42] M. Górka, *Przywództwo charyzmatyczne księdza Jerzego Popiełuszki*, „Zeszyty Naukowe Almmamer", 2011, nr 64/2, s. 245–259.

[43] M. Górka, *Leopold Tyrmand – kontestator komunizmu. Rzeczywistość dekady stalinowskiej w zwierciadle Dziennika 1954 oraz prasy PRL*, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2014.

[44] *U brzegów Leopolda Tyrmanda*, red. M. Górka, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2015.

wyjścia do konfrontacji zapisów prowadzonych przez pisarza z oficjalnymi artykułami publikowanymi w prasie codziennej, jak: „Życie Warszawy", „Express Wieczorny" i „Trybuna Ludu", dzięki czemu możliwe staje się zbadanie zjawiska propagandy z lat 50. W ten sposób prezentowane książki stanowią wyjątkowy charakter w dotychczasowej literaturze przedmiotu, wzbogacając o nową wiedzę również obszar nauk o polityce.

Ważnym osiągnięciem w zakresie rozwoju naukowego są redakcje prac zbiorowych (16 publikacji). Do najważniejszych z nich można zaliczyć: *Rola i zadania służb w systemie bezpieczeństwa publicznego*[45]; *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa*[46]; *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*[47]. Ich pełna lista znajduje się w załączniku nr 4c (pt. Wykaz dorobku habilitacyjnego – nauki społeczne).

W toku działalności naukowej przygotowane zostały dwie recenzje wydawnicze. Pierwsza dotyczy monografii pt. *Indochiny w amerykańskiej polityce powstrzymania do 1963 roku*[48], druga odnosi się do pracy zbiorowej pt. *Polska – Europa – Świat. Wczoraj i dziś*[49].

W dorobku naukowym znajdują się także dwie recenzje książek, opublikowane w polskich czasopismach naukowych i są to: *Unia Europejska w stosunkach międzynarodowych*[50] oraz *Cyfrowe dzieci. Zjawisko, uwarunkowania, kluczowe problemy*[51].

Na pracę naukową składają się również referaty wygłoszone podczas zagranicznych konferencji naukowych:

1. The Third International Congress of Belarusian Studies, tytuł referatu: *Carnivalesque Elements in Protests of Belarusian Opposition*, Kowno (Litwa), październik 2013 r.
2. The Fourth International Congress of Belarusian Studies, tytuł referatu: *Selected Determinants of Activity of Special Services in the Region of Central and Eastern Europe,* Kowno (Litwa), 3–5 października 2014 r.

---

[45] *Rola i zadania służb w systemie bezpieczeństwa publicznego*, red. M. Górka, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2013.

[46] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa*, red. M. Górka, Warszawa: Wydawnictwo Difin 2014.

[47] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa,* red. M. Górka, Warszawa: Wydawnictwo Difin 2017.

[48] M. Adamczyk, O. Szuflet, *Indochiny w amerykańskiej polityce powstrzymania do 1963 roku*, Poznań: Wydawnictwo Media Expo 2017.

[49] *Polska – Europa – Świat. Wczoraj i dziś*, red. M. Debita, M. Adamczyk, Poznań: Wydawnictwo Media Expo 2017.

[50] *Unia Europejska w stosunkach międzynarodowych*, red. M. Rewizorski [w:] „Stosunki Międzynarodowe – International Relations", 2012, nr 45/1, s. 313–317.

[51] *Cyfrowe dzieci. Zjawisko, uwarunkowania, kluczowe problemy*, red. S. Bębas, A. Szwedzik, M.Z. Jędrzejko, K. Kasprzak, A. Taper, Wydawnictwo Aspra, Warszawa – Milanówek 2017, s. 396, „Studia Edukacyjne", 2017, nr 3, s. 445–447.

3. Jont Interdisciplinary Conferences. The 5th International Symposium on Art./Science/Technology MEDEA'2017; tytuł referatu: *Cyber technology – Opportunity or Threat for the Development of Public Institutions*, 1–8 września 2017, Heraklion, Grecja
4. Jont Interdisciplinary Conferences. The 5th International Symposium on Art./Science/Technology MEDEA'2017; prowadzenie warsztatów: *Manipulation Techniques on the Internet. How to Spot a Liar in Cyberspace?*, 1–8 września 2017, Heraklion, Grecja
5. 23rd Annual Conference of Central European Political Science Association, tytuł referatu: *The Three Seas Initiative as a new challenge for the ECE countries*, 13–14 września 2018, Banská Bystrica, Słowacja

Oprócz tego byłem moderatorem panelu pt. *Wywiad i kontrwywiad jako narzędzie zmiany polityki państwa* podczas IV Ogólnopolskiego Kongresu Politologii w Lublinie w dniach 19–20.09.2018 r. Pełną listę wygłoszonych referatów na międzynarodowych i krajowych konferencjach zawiera załącznik nr 4c (pt. Wykaz dorobku habilitacyjnego – nauki społeczne).

Kolejnym ważnym krokiem w rozwoju zainteresowań badawczych nad polityką bezpieczeństwa w Europie Środkowej był udział w międzynarodowym projekcie naukowym pod tytułem „Visegrad Group and the Central European Cooperation" (No. 61450025) finansowanym przez Międzynarodowy Fundusz Wyszehradzki. Praca w międzynarodowym zespole umożliwiła pozyskanie trudno dostępnych danych na temat cyberzagrożeń występujących wśród państw Grupy Wyszehradzkiej. Efektem badań w zespole był także udział w publikacji monografii naukowej pt. *Security, Foreign and European Policy of the Visegrad Group*[52].

Kontynuacją podjętych działań naukowych było również uczestnictwo w Międzynarodowej Konferencji organizowanej przez Europejskie Stowarzyszenie Nauk Politycznych (23rd Annual Conference of Central European Political Science Association – One hundred years after, 1918–2018). Podczas tego wydarzenia zaprezentowane były wyniki badań z zakresu polityki cyberbezpieczeństwa państw Trójmorza.

Dużą wartością dla rozwoju naukowego w obszarze badań nad polityką bezpieczeństwa jest praca w zespole badawczym *Italian Team for Security, Terroristic Issues & Managing Emergencies*. Zarówno polskie, jak i zagraniczne publikacje były przygotowywane na

[52]*Security, Foreign and European Policy of the Visegrad Group*, red. L. Cabada, Š. Waisová, Metropolitan University Prague Press and Togga, Praga 2018.

podstawie licznych konsultacji w ramach pracy w tym zespole. Dodatkowo współpraca stanowiła okazję do omawiania oraz publikowania materiałów dotyczących wydarzeń politycznych w Polsce, czego przykładem są m.in. takie publikacje jak: *Polish politics: a conservative revolution or post-democracy?*[53] oraz *Poland and Israel: difficult relations between two friends*[54].

Ponadto od 2016 roku jestem członkiem Polskiego Towarzystwa Oceny Technologii oraz Polskiego Towarzystwa Geopolitycznego.

Znaczącym sukcesem w dotychczasowej pracy naukowej była nagroda przyznana przez redakcję Kwartalnika Naukowego OAP UW „e-Politikon" za artykuł pt. *The Meme as an Example of Carnivalized Internet Communication*[55].

Pragnę zaznaczyć, że w latach 2012–2018 otrzymałem również sześciokrotnie nagrodę indywidualną JM Rektora Politechniki Koszalińskiej za działalność naukową oraz trzykrotnie za działalność organizacyjną.

Ważnym obszarem aktywności naukowej jest praca w komitetach redakcyjnych i radach naukowych takich czasopism, jak: „Politics in Central Europe" (vol. 14/1, 2018; vol. 14/3, 2018), „Symbolae Europaeae" (nr 11, 2017; nr 12, 2017; nr 13, 2018), „Racja Stanu" (nr 17/1, 2015; nr 18–19, 2016).

5.1. Działalność dydaktyczna i organizacyjna

Oprócz wykładów i ćwiczeń w ramach programu studiów na kierunku europeistyka na Wydziale Humanistycznym Politechniki Koszalińskiej prowadziłem także wykłady dla studentów Instytutu Socjologii na Katolickim Uniwersytecie Lubelskim Jana Pawła II z zakresu polityki cyberbezpieczeństwa. Ponadto realizowane były również wykłady na temat cyberbezpieczeństwa dla członków Polskiego Towarzystwa Ekonomicznego.

W latach 2011–2017 prowadzone były lekcje dla uczniów wielu szkół na temat „bezpieczeństwa na portalach społecznościowych". Aktywność dydaktyczna zaowocowała licznymi projektami i współpracą z jednostkami edukacyjnymi, czego przykładem jest wykonanie ekspertyzy dla Przedsiębiorstwa Organizacji Wdrożeń „AYA" Spółka z o.o. w

---

[53] M. Górka, *Polish politics: a conservative revolution or post-democracy?*, źródło: http://www.itstime.it/w/polish-politics-a-conservative-revolution-or-post-democracy-marek-gorka (dostęp: 12.04.2018).

[54] M. Górka, *Poland and Israel: difficult relations between two friends*, źródło: http://www.itstime.it/w/poland-and-israel-difficult-relations-between-two-friends-by-marek-gorka (dostęp: 12.04.2018).

[55] M. Górka, *The Meme as an Example of Carnivalized Internet Communication*, op. cit.

zakresie skutecznych działań edukacyjnych wobec cyberzagrożeń wśród młodzieży szkolnej. Mój wkład w powstanie tego raportu polegał na kierowaniu zespołem eksperckim oraz opracowaniu wyników.

Pełniłem funkcję promotora pomocniczego w przewodzie doktorskim mgr. Krzysztofa Kaczmarka. Przewód doktorski został otwarty decyzją Rady Wydziału Humanistycznego Uniwersytetu Szczecińskiego 22 września 2017 roku. Promotorem rozprawy został dr hab. Ryszard Tomczyk, prof. US. 22 maja 2018 roku odbyła się publiczna obrona rozprawy doktorskiej pt. *Proces europeizacji Finlandii ze szczególnym uwzględnieniem Laponii. Doświadczenia społeczno-gospodarcze.*

W ramach seminarium magisterskiego na kierunku europeistyka prowadzonego na Wydziale Humanistycznym Politechniki Koszalińskiej byłem promotorem 89 prac magisterskich.

W obszarze działalności dydaktycznej w latach 2012–2017 byłem również opiekunem Politologicznego Koła Naukowego na Wydziale Humanistycznym Politechniki Koszalińskiej. Aktywność ta zaowocowała licznymi konferencjami naukowymi na temat m.in.: *Przywódcy Solidarności* (2012); *Młodzi i Polityka* (2013); *Bezpieczeństwo publiczne. Analiza sytuacji lokalnej* (2013); *Terroryzm i antyterroryzm w XXI wieku* (2014); *Ochrona socjalna społeczeństwa – administracja – innowacja* (2014); *Społeczno-administracyjny wymiar systemu bezpieczeństwa publicznego* (2015). Efektem tych działań jest również udział studentów w publikowanych pracach naukowych, jak: *Solidarność: Ludzie i idee*[56], red. M. Górka, Koszalin 2012, *Rola i zadania służb w systemie bezpieczeństwa publicznego*[57], red. M. Górka, Koszalin 2013, *Młodzi i Polityka*[58], red. M. Górka, J. Prokopiuk, Koszalin 2013; *Teoretyczne i praktyczne aspekty polityki bezpieczeństwa publicznego*[59], red. M. Górka, G. Tokarz, Koszalin 2015.

5.2. Popularyzacja nauki

Na proces popularyzacji nauki składa się uczestnictwo w audycjach radiowych i telewizyjnych na temat aktualnych wydarzeń politycznych. Ponadto nawiązana została współpraca z prasą lokalną, w której ramach publikowane były wywiady, komentarze oraz

[56] *Solidarność. Ludzie i idee*, red. M. Górka, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2012.

[57] *Rola i zadania służb w systemie bezpieczeństwa publicznego*, red. M. Górka, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2013.

[58] *Młodzi i Polityka*, red. M. Górka, J. Prokopiuk, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2013.

[59] *Teoretyczne i praktyczne aspekty polityki bezpieczeństwa publicznego*, red. M. Górka, G. Tokarz, Koszalin: Wydawnictwo Politechniki Koszalińskiej 2015.

artykuły publicystyczne na temat polityki lokalnej, rywalizacji wyborczej oraz polityki bezpieczeństwa. Opublikowany został również artykuł w czasopiśmie ogólnopolskim na temat działalności służb izraelskich w zakresie antyterroryzmu[60].

W ramach aktywności popularyzującej badania naukowe pełnione były obowiązki koordynatora Zachodniopomorskiego Festiwalu Nauki na Politechnice Koszalińskiej; ponadto prowadzone były wykłady pt. *Mowa nienawiści – realny i wirtualny problem społeczny* w Koszalińskiej Bibliotece Publicznej, a także w ramach programu *Noc szkoleń* realizowane były warsztaty pt. *Innowacyjna edukacja w epoce cyberzagrożeń. Jak się nie dać oszukać w Internecie*.

Ważnym wydarzeniem była organizacja *Nocy wyborczej* dotyczącej wyborów prezydenckich w USA w 2016 roku odbywającej się w Radiu Koszalin. Okazją do popularyzowania nauki było również uczestnictwo w debatach radiowych na temat współczesnego patriotyzmu pt. *Znaki wolności, lustra niepodległości* oraz debaty organizowane przez Szkołę Liderów pt. *Kadencyjność, dobra czy zła zmiana?*

W ramach kształtowania świadomości społecznej oraz postaw obywatelskich realizowane były liczne wystąpienia naukowe podczas *Wieczornic Historycznych* odbywających się na Wydziale Humanistycznym Politechniki Koszalińskiej, a aktywność w zakresie popularyzacji historii najnowszej została doceniona przez Radę Ochrony Pamięci Walk i Męczeństwa nadaniem Srebrnego Medalu Opiekuna Miejsc Pamięci Narodowej.

Marek Górka

[60] M. Górka, *Działalność służb izraelskich w zakresie antyterroryzmu*, „Antyterroryzm. Polska i Świat", 2017, nr 1, s. 14–17.