Banasik, M., Chojnowski, L., 2024. *Rywalizacja strategiczna w cyberprzestrzeni i jej konsekwencje dla bezpieczeństwa międzynarodowego,* Przegląd Geopolityczny, 48, s. 69-90.

Mirosław BANASIK
Akademia Piotrkowska
ORCID: 0000-0002-9358-1240
Lech CHOJNOWSKI
Uniwersytet Pomorski w Słupsku
ORCID: 0000-0003-0339-0430

RYWALIZACJA STRATEGICZNA W CYBERPRZESTRZENI I JEJ KONSEKWENCJE DLA BEZPIECZEŃSTWA MIĘDZYNARODOWEGO

STRATEGIC COMPETITION IN CYBERSPACE AND ITS IMPLICATIONS FOR INTERNATIONAL SECURITY

Abstract:
The purpose of the research was to clarify the mechanisms of strategic competition, including in cyberspace, and to identify the challenges and threats arising from it for international security. Literature analysis and criticism, non-participatory observation and case studies were used to solve the research problems. In the research process, it was determined that in the next decade the strategic competition will be most intense between the United States, and China and the Russian Federation. The biggest threats to the existing international order will be the ambitions of revisionist states related to territorial claims and expansion of spheres of influence. These states will use mainly non-military instruments of influence, including cyberspace, to gain an advantage over competing societies. Cyberspace will not only be the main pillar of competition, but also an alternative to it.

Keywords: strategic competition, international security, cyberspace, China, United States, Russian Federation, challenges and threats.

Wstęp

Rywalizacja strategiczna pomiędzy wielkimi mocarstwami jest głęboko zakorzeniona w historii. Termin wielkie mocarstwo po raz pierwszy wszedł do języka dyplomatycznego w czasach wojen napoleońskich. Pierwsze próby podjęte przez naukowców opracowania formalnych kryteriów definiujących państwa wywierające wyraźny wpływ na system międzynarodowy koncentrowały się na potędze militarnej. Później uwzględniano również potencjał ludzki, gospodarczy i

polityczny. Chociaż trudno jest obecnie dostrzec konsensus definicyjny to wydaje się, że dwa dodatkowe kryteria są wspólne dla wszystkich opracowań teoretycznych. Wielkie mocarstwo postrzega swoje interesy w kategoriach kontynentalnych, lub globalnych i posiada zdolności do projekcji siły poza własnymi granicami. Aby być wielkim mocarstwem, państwo musi być również uznawane za takie przez inne państwa w systemie międzynarodowym (Evans, 2023, s. 1). Charakter rywalizacji strategicznej między mocarstwami na przestrzeni wieków ulegał zmianom, ale trudno jest dostrzec typowe analogie tych zmian. W czasach zimnej wojny rywalizacja pomiędzy Stanami Zjednoczonymi Ameryki (USA), a Związkiem Socjalistycznych Republik Radzieckich koncentrowała się na maksymalnym powstrzymaniu państwa sowieckiego przed dominacją w wymiarze politycznym, ekonomicznym, ideologicznym i militarnym. Z kolei Związek Radziecki dążył do przesunięcia na własną korzyść korelacji sił zbrojnych (Raska, 2020, s. 66), dążąc w ten sposób do osiągnięcia przewagi strategicznej. W XXI wieku rywalizacja strategiczna stała się bardziej złożona, nieprzewidywalna i zróżnicowana. Gwałtownie przebiegające zjawiska w relacjach międzynarodowych, a szczególnie pomiędzy wielkimi mocarstwami, świadczą o tym, że świat wkroczył w nową erę międzypaństwowej rywalizacji strategicznej, aczkolwiek do końca nie wiadomo jakie będą jej konsekwencje. Największe obawy pojawiają się w związku z narastającą konkurencją polityczną, gospodarczą i militarną. W polityce zagranicznej Stanów Zjednoczonych Ameryki następuje zmiana paradygmatu zapewniania bezpieczeństwa, który do tej pory koncentrował się na podmiotach pozapaństwowych i wyrażał się angażowaniem w konflikty o niskiej intensywności (White, 2017, s. 2, U.S. Department, 2018). Zmiana amerykańskich priorytetów została podyktowana autorytarnym modelem sprawowania władzy przez Chiny i Rosję, co prowadzi do osłabienia obowiązującego porządku międzynarodowego i wywołuje negatywne konsekwencje dla stabilności bezpieczeństwa. Ponadto gwałtowny rozwój nowoczesnych technologii pozwolił na intensyfikację rywalizacji strategicznej i jej przenoszenie w cyberprzestrzeń.

Rywalizacja strategiczna odbywa się w wielu sferach oddziaływania, na różnych poziomach i w wielu domenach operacyjnych. Jeśli chodzi o rywalizację w skali globalnej to kluczową rolę w osiąganiu dominacji nad rywalem nadal odgrywa siła militarna (Gürer, 2021). Jednak coraz większe znaczenie w jej prowadzeniu ma sfera informacyjna, a w niej cyberprzestrzeń. Twarda siła w rywalizacji o

władzę nie traci na znaczeniu, niemniej jednak oddziaływanie z wykorzystaniem siły miękkiej jest o wiele bardziej dostępne i mniej kosztowne, co pozwala państwom nieposiadającym dostatecznych zasobów militarnych na uzyskanie wyraźnej przewagi nad rywalem strategicznym. Osiąganie celów strategicznych przy pomocy instrumentów miękkiego oddziaływania, co potwierdziły doświadczenia konfliktów ostatniej dekady, jest bardziej skuteczne niż przy pomocy instrumentów twardego oddziaływania. Ponadto może się odbywać w dłuższym czasie i czasami jest trudne do wykrycia, szczególnie jeśli odbywa się w cyberprzestrzeni (Bagińska, 2018, s. 11). Wynika z tego, że zagrożenia o charakterze niemilitarnym wywierają określoną presję na rywala strategicznego, a ich zakres może wykraczać poza pojedyncze państwo. Oznacza to, że mogą one mieć charakter regionalny, a nawet globalny (Gürer, 2021).

Na podstawie badań wstępnych ustalono, że państwa oddziałują na rywali strategicznych w sposób kompleksowy. Oznacza to, że rywalizacji strategicznej nie należy postrzegać przez pryzmat odrębnych domen, w których walczy się o uzyskanie dominacji. Ze względu na pojawiającą się nową przestrzeń prowadzonej rywalizacji, jaką staje się cyberprzestrzeń, współcześnie należy wychodzić nawet dalej, niż traktowanie domen w sposób łączny, w ramach prowadzenia operacji połączonych. Cyberprzestrzeń umożliwia prowadzenie operacji w innych domenach, dlatego też nie należy jej zbyt pochopnie traktować odrębnie. Dzięki cyberprzestrzeni, podobnie jak w innych domenach rywalizacji, można prowadzić odstraszanie i wymuszania, a także osiągać pożądane efekty zarówno w sferze kinetycznej, jak i niekinetycznej (Shea, 2018, s. 137). Ponadto postrzeganie cyberprzestrzeni jako odrębnej domeny może prowadzić do niedostrzeżenia implikacji konwergencji zagrożeń w cyberprzestrzeni z zagrożeniami pochodzącymi z innych domen, co może mieć konsekwencje osłabienia zdolność do powstrzymywania i obrony przed przeciwnikiem wykorzystującym luki i słabości w coraz bardziej współzależnych systemach obronnych i infrastrukturze państwa. Poza tym należy brać pod uwagę fakt, że technologie integrują zarówno systemy funkcjonujące w ramach odrębnych domen, jak i poszczególne domeny. Dla przykładu platformy i systemy bezpieczeństwa coraz częściej stanowią część złożonego, usieciowionego ekosystemu, wyróżniającego się kompleksowością (Joine, Tutty, 2018), a dzięki cyberprzestrzeni możliwe jest osiąganie pożądanych efektów wielodomenowych (Framework, 2018, s. 5).

Należy jednak wyraźnie zaznaczyć, że cyberprzestrzeń charakteryzuje się określoną specyfiką i znacznie różni się od naturalnie ograniczonych domen przestrzeni powietrznej, lądowej, morskiej i kosmicznej. Jej specyficznymi cechami są globalny zasięg wykorzystanie spektrum elektromagnetycznego, a także anonimowość i aterytorialność (Marczyk, 2018, s. 60). Cyberprzestrzeń wzmacnia interakcje międzydomenowe i posiada cechy adaptacyjności (Olagbemiro, 2014, s. 14). Działania w cyberprzestrzeni ułatwiają operowanie w innych domenach. I na odwrót, aktywności w innych domenach mogą wywoływać efekty w cyberprzestrzeni (Kuusisto, 2015, s. 35), bądź za jej pośrednictwem w świecie rzeczywistym (Air Force, 2023, s. 2). Operacje w cyberprzestrzeni mogą być prowadzone niezależnie lub być synchronizowane i integrowany z klasycznymi zdolnościami operacyjnymi, w celu zwiększenia skuteczności oddziaływania (Air Force, 2023, s. 2). Oznacza to, że cechy strukturalne cyberprzestrzeni umożliwiają aktorom działanie w sposób nieosiągalny w innych domenach konwencjonalnych (Harknett, Smeets, 2020, s. 10). Poza tym powiązania międzydomenowe pozwalają na wywieranie wpływu na rywala strategicznego w znacznym oddaleniu i wywoływanie pożądanych efektów strategicznych bez potrzeby angażowania się w wymiarze fizycznym.

Mimo to, że literatura coraz częściej koncentruje się na ocenie cyberprzestrzeni w kontekście politycznym, strategicznym i prawnym, co oznacza dążenia do wychodzenia poza ramy konfliktu zbrojnego toczonego w tej domenie (Friis, Ringsmose, 2016) oraz uwzględnianiu preferencji strategicznych (Gomez, 2023), to ograniczone są opracowania koncentrujące się na operacjonalizacji mechanizmów prowadzenia rywalizacji strategicznej i ich konsekwencjach dla bezpieczeństwa międzynarodowego, co sprawia, że w tym obszarze występuje określona luka poznawcza. Szczególnie odnosi się to do prowadzenia rywalizacji w cyberprzestrzeni, która zapewnia możliwość oddziaływania strategicznego poniżej granicy bezpośredniego konfliktu zbrojnego. Wynika z tego, że problematyka bezpieczeństwa międzynarodowego rozpatrywana przez pryzmat rywalizacji strategicznej w cyberprzestrzeni jest jeszcze niewystarczająco zbadana i opisana, szczególnie w zakresie wyzwań i zagrożeń jakie ze sobą niesie. Ponadto określone trudności wynikają z przewidywania zakresu i intensywności konfliktów w cyberprzestrzeni i brak jest mechanizmów pozwalających na obiektywną ich ocenę. Trudno też jest poprawnie identyfikować i oszacować efekty, które mogą mieć miejsce w świecie

rzeczywistym w rezultacie oddziaływania w cyberprzestrzeni. Nie są jasne zależności występujące pomiędzy konfliktami w cyberprzestrzeni, a konfliktami konwencjonalnymi, co sprawia występowanie poważnych dwuznaczności w ocenach ich potencjalnych implikacji strategicznych. Ponadto międzynarodowe regulacje prawne nie są dostosowane do wymagań prowadzenia konfliktów w cyberprzestrzeni (Kosenkov , 2016, s. 3).

Na podstawie występującej luki poznawczej sformułowano główny problem badawczy, który brzmi: *Jakie wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego niesie za sobą rywalizacja strategiczna?* Główny problem badawczy poddano fragmentacji i określono następujące problemy szczegółowe:

1) Jaka jest istota i charakter rywalizacji strategicznej oraz jakie mogą być jej konsekwencje?

2) W czym wyraża się specyfika rywalizacji w cyberprzestrzeni i jakie niesie ona za sobą wyzwania i zagrożenia dla bezpieczeństwa?

Celem badań było wyjaśnienie mechanizmów prowadzenia rywalizacji strategicznej, w tym w cyberprzestrzeni oraz zidentyfikowanie wyzwań i zagrożeń z niej wynikających dla bezpieczeństwa międzynarodowego, a także rekomendacji dla decydentów polityczno-militarnych. Aby ukierunkować proces badawczy, sformułowano hipotezę badawczą wyrażającą się przypuszczeniem, że obecnie zaostrza się rywalizacja strategiczna pomiędzy globalnymi aktorami, która jest głównym wyzwaniem dla utrzymania stabilności bezpieczeństwa międzynarodowego. Intensywność tej rywalizacji wyraża się mocarstwowymi ambicjami Federacji Rosyjskiej, dążącej do zmiany aktualnie obowiązującego ładu międzynarodowego i Chin prowadzących rywalizację strategiczną w szarej strefie. Rywale strategiczni dążą do odnoszenia sukcesów bez potrzeby bezpośredniego konfliktu zbrojnego. Szczególną w tym rolę odgrywa cyberprzestrzeń, dzięki której możliwe staje się integrowanie wszystkich możliwych domen oddziaływania strategicznego i kreowania warunków do osiąganie pożądanych celów politycznych na arenie międzynarodowej.

W procesie badawczym przyjęto założenie, że rywalizacja strategiczna jest prowadzona przy pomocy instrumentów znajdujących się w dyspozycji pastwa, które tworzą ściśle uporządkowany system oddziaływania na stronę przeciwną. Dlatego też do badania oddziaływań, współzależności i związków pomiędzy mechanizmami oddziaływania strategicznego a uczestnikami środowiska

bezpieczeństwa międzynarodowego i zidentyfikowania konsekwencji tego oddziaływania zastosowano podejście systemowe. W oparciu o nie badane były wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego. W rozwiązywaniu problemów badawczych i uzyskaniu obiektywnych danych jakościowych zastosowano głównie analizę i krytykę literatury, obserwację nieuczestniczącą oraz studium przypadków. Pomocną również była analiza porównawcza i uogólnienie, które pozwoliły na wyznaczenie trendów i mechanizmów, stosowanych do osiągania celów rywalizacji strategicznej oraz ich implikacji dla bezpieczeństwa międzynarodowego. Przedstawione w artykule wnioski są wynikiem zastosowania rozumowania indukcyjnego i dedukcyjnego.

Istota, charakter i konsekwencje rywalizacji strategicznej

Na przełomie drugiej i trzeciej dekady XXI wieku świat wkroczył w nową erę wzmożonej rywalizacji strategicznej, charakteryzującej się konfrontacją polityczną, ekonomiczną i militarną. Rywalizacja ta może zwiastować długi okres niepewności, ograniczania stabilności bezpieczeństwa oraz zmiany obowiązującego stanu porządku międzynarodowego. Chiny i Federacja Rosyjska coraz wyraźniej manifestują niezadowolenie z obowiązującego ładu międzynarodowego i podejmują aktywne działania na rzecz jego zmiany, dążąc do ukształtowania świata zgodnego z własnym, autorytarnym modelem sprawowania władzy. Rewizjonistyczne ambicje Kremla doprowadziły do wojny z Ukrainą[1], a Chin wyrażają się przejmowaniem terytoriów na Morzu Południowochińskim. Oba państwa dążą do powiększania własnych stref wpływów, daleko wykraczających poza ich granice. Dynamika zjawisk zachodzących pomiędzy państwami, a szczególnie wielkimi mocarstwami jest wysoka, dlatego trudno jest przewidywać konsekwencje działań podejmowanych w ramach rywalizacji

[1] Inwazja Federacji Rosyjskiej na Ukrainę dokonana 24 lutego 2022 roku spowodowała wstrząs w systemie międzynarodowym. Jak podkreślają eksperci nie można wykluczyć w tym konflikcie użycia broni nuklearnej. Reakcja Zachodu obecnie jest skoncentrowana na udzielaniu pomocy wojskowej dla Ukrainy i stosowaniu sankcji gospodarczych przeciwko Rosji. Konsekwencje wojny są daleko idące i mogą mieć zasięg globalny. Ograniczenie eksportu tych dwóch największych producentów żywności ma poważny wpływ na światowe bezpieczeństwo żywnościowe. Zmieniane są europejskie priorytety dotyczące bezpieczeństwa. Zmianom też ulegają globalne układy polityczne i preferencje strategiczne. Sprzeciw wobec działań Rosji na Ukrainie był powszechny, ale nie całkowity. W marcu 2022 roku w trakcie głosowania nad rezolucją potępiają agresję Rosji aż 35 państw wstrzymało się od głosu. Również wstrzymały się od głosowania Chiny, które potwierdziły tym samym bliską przyjaźń z Federacją Rosyjską (SIPRI, 2022, s. 1).

strategicznej i z jednej strony jednoznacznie ustalić, jaki będzie ich wpływ na degradację środowiska strategicznego, a z drugiej strony precyzyjnie określić, jakie będą możliwości zapewnienia stabilności bezpieczeństwa międzynarodowego w przyszłości.

W znaczeniu potocznym rywalizacja to współzawodnictwo i dążenie do zdobycia pierwszeństwa w osiągnięciu czegoś (Kamińska-Szmaj 2001, s. 711). W relacjach międzynarodowych chodzi głównie o środki służące do zaspakajania potrzeb państwa. Są one z reguły ograniczone, co sprawia, że trzeba o nie zabiegać. Z rywalizacją możemy mieć do czynienia wszędzie tam, gdzie ludzie mają ten sam lub podobny cel i chcą go osiągnąć szybciej, bądź lepiej niż rywale (Dubisz, 2006, t. 2, s. 209). W takiej sytuacji zazwyczaj występuje presja konkurencyjna, co bardzo często obserwuje się w ekonomii (The Concept, 2021, s. 9). W sytuacji rywalizacji pomiędzy ludźmi o przeciwstawnych potrzebach, przekonaniach, wartościach lub celach dochodzi do konfliktu, który w najszerszym ujęciu oznacza niezgodność stanowisk. Otwartą kwestią pozostaje charakter tych niezgodności, tj. czy występują one między jednostkami, grupami lub społeczeństwami, czy wynikają z różnych interesów lub przekonań, czy mają podłoże materialne, lub czy powstają tylko w sferze narracji (Pia, 2006, s. 2). Mimo to należy uznać, że rywalizacja jest intensywną formą konkurencji, w której występują pewne antagonizmy, ale poziom wzajemnej wrogości może być różny. Ponadto jej celem jest uzyskanie określonych korzyści materialnych bądź niematerialnych.

W trakcie rywalizacji bardzo często dochodzi do kontestacji, która w ogólnym znaczeniu oznacza sprzeciw osoby albo grupy przeciwko funkcjonującym w społeczeństwie normom i zasadom. Chodzi tu o kwestionowanie wartości i norm obowiązujących w życiu społecznym, a przede wszystkim politycznym (Satkiewicz, 1994, s. 10). Kontestacja to dezaprobata, przeciwstawianie się czemuś lub komuś, opór i w końcu walka. Walka ta może przybierać formę agresji werbalnej lub niewerbalnej (Święcicka, 2014). W wymiarze politycznym kontestacja była bardzo mocno dostrzegalna w drugiej dekadzie XXI wieku, co wyrażało się kwestionowaniem granic terytorialnych, obowiązującego porządku bezpieczeństwa i ładu oraz prawa międzynarodowego i bezpośrednio prowadziło do powstawania sporów, konfliktów, a nawet wojen.

Rywalizacja może być też rozumiana jako stan, w którym państwo globalnie dąży do maksymalizacji swojej względnej przewagi nad innym wielkim mocarstwem (Deconstructing, 2021, s. 18). Rywalizacja nie

wyklucza jednak współpracy. W związku z tym należy ją rozpatrywać przez pryzmat celów działania państw, jakimi są określone korzyści. W przypadku współpracy korzyści dotyczą obydwu stron, natomiast w przypadku rywalizacji chodzi głównie o zmniejszenie korzyści strony konkurencyjnej (Milner, 1992, s. 46). Chodzi o takie zachowania, których konsekwencje będą szkodliwe dla interesów drugiej strony, szczególnie tych postrzeganych jako priorytetowe. Jeśli okaże się, że priorytety są trudne do osiągnięcia lub są nieopłacalne z punktu widzenia ich osiągania, gdyż może to doprowadzić do starcia zbrojnego, to wówczas podmiot rywalizujący może się zdecydować na przejście do szarej strefy[2]. Ważne podkreślenia jest celowe oddziaływanie, szkodliwe dla żywotnych interesów strony przeciwnej[3]. Przeciwstawne zamiary strategiczne mogą się ujawnić w dłuższym czasie, co oznacza dla przykładu, że suma pozornie łagodnego oddziaływania może poprzez kumulowanie się określonych efektów w czasie zmienić środowisko bezpieczeństwa w sposób sprzeczny z interesami konkurenta (Burkhart, Woody, 2017, s. 24). Uogólniając, można przyjąć, że rywalizacja może być rozumiana jako stan antagonistycznych relacji, ale nie jest

[2] Oddziaływanie w szarej strefie w literaturze bardzo często nazywane jest wojną w szarej strefie. Termin wojny w szarej strefie oznacza też celowe, wielowymiarowe oddziaływanie państwa poniżej granicy agresywnego użycia sił zbrojnych. W tego typu konfliktach, w opinii F. Hoffmana, stosuje się w sposób zintegrowany szereg narodowych i regionalnych instrumentów oddziaływania i dzięki dwuznacznościom, operując poniżej progu otwartego konfliktu, osiąga się specyficzne cele strategiczne. Dla zwiększenia skuteczności oddziaływania siły militarnej stosuje się pododdziały zastępcze bez wyraźnych oznak przynależności państwowej, co uniemożliwia ich zdemaskowanie (Hoffman, 2016, s. 26). Nieco inaczej wojnę w szarej strefie pojmuje Phillip Kapusta. Jego definicja odnosząca się do wyzwań wynikających z szarej strefy jest bardziej ogólna i obejmuje również podmioty niepaństwowe. W rozumieniu P. Kapusty szara strefa obejmuje konkurencyjne oddziaływania pomiędzy i w granicach państw oraz aktorów niepaństwowych zawierające się pomiędzy dwoistością wojny a pokoju. Ta dwoistość jest przyczyną dwuznaczności. Dwuznaczności wynikają z charakteru konfliktu, braku pewności co do zaangażowanych aktorów, polityki i aspektów uregulowań prawnych Kapusta, 2015, s. 20.

[3] Dyplomatyczne akty rywalizacji mogą obejmować szpiegostwo i sabotaż. Operacje informacyjne mogą obejmować techniki decepcji i dezinformacji oraz propagandę. Militarny aspekt oddziaływania mogą obejmować wojnę zastępczą, taktykę partyzancką, tajne operacje lub mieszankę tajnych i jawnych operacji. Działania gospodarcze w ramach rywalizacji mogą przybierać formę sankcji, barier handlowych lub taryf. Rywalizacja bardzo często przybiera charakter asymetryczny wyrażający się działaniami przestępczymi, stosowanymi dla odnoszenia określonych korzyści politycznych, a także może być stosowany terroryzm lub aneksja obcych terytoriów. Rywalizacja jest prowadzona bardzo często w sposób skryty, niejednoznaczny, stopniowy, pośredni lub jako połączenie wszystkich wymienionych form oddziaływania (Burkhart, Woody, 2017, s. 24).

bezpośrednim konfliktem zbrojnym, rozumianym jako walka pomiędzy stronami o przeciwstawnych celach, wartościach lub przekonaniach, co z kolei może prowadzić do jawnej konfrontacji militarnej lub działań wojennych (Deconstructing, 2021, s. 18).

Rywalizację można traktować jako próbę zdobycia przewagi nad innymi, rozumianą jako egoistyczną pogoń za takimi dobrami jak władza, bezpieczeństwo, bogactwo, wpływy i status (Mazarr i inni, 2018, s. 5). Dążenia do pozyskania tych dóbr zazwyczaj generuje wyzwania i zagrożenia dla bezpieczeństwa lokalnego i regionalnego. Rywalizację postrzeganą z szerszej perspektywy, należy rozumieć jako dążenia do osiągnięcia globalnego przywództwa, co wiąże się z decydowaniem o rozstrzyganiu sporów międzynarodowych i ma swoje konsekwencje dla globalnego środowiska bezpieczeństwa. W rozstrzyganiu określonych roszczeń stale jest obecna groźba lub ma miejsce rzeczywiste użycie siły militarnej, co wiąże się z koniecznością wrogich interakcji (Hensel, 1999, s. 4). W opinii P.F. Diehla i G. Goertza (2006, s. 339) rywalizacji zawsze towarzyszy użycie siły, natomiast dla D. Scotta Bennetta nie jest ona kluczowa (Bennet, 1996, s. 166).

Posługiwanie się w relacjach międzynarodowych atrybutem siły może świadczyć o występowaniu rywalizacji militarnej. Nie ma jednak konsensusu co do tego, jak bardzo zmilitaryzowane muszą być relacje, zanim zostaną one uznane za rywalizację (Mazarr, 2021, s. 7). Nasilające się różnorodne formy wrogości wiąże się z dużym prawdopodobieństwem użycia siły, w tym oczywiście z wojną na pełną skalę. Należy jednak zauważyć, że rywalizacja może mieć miejsce tylko pomiędzy państwami o mniej więcej równych potencjałach, ale nie może być mowy o rywalizacji pomiędzy państwami w sytuacji, w której występują duże dysproporcje siły, a szczególnie w posiadanych zdolnościach militarnych. Państwo dominujące nie musi rywalizować ze słabszym przeciwnikiem, ponieważ istnieje niewielka szansa, że słabsze państwo w niej zwycięży (Vasquez, 1996, s. 533). Większość badaczy nie odrzuca jednak zjawiska rywalizacji asymetrycznej (Soon-Kun, s. 242 i Mundt, Oh, 2019).

Problemy zagrożeń dla bezpieczeństwa międzynarodowego wynikające ze strategicznej rywalizacji zostały wyraźnie wyartykułowane w nowej koncepcji strategicznej NATO (2022), strategiach bezpieczeństwa narodowego największych państw świata oraz wielu państw europejskich. Najważniejsze państwa europejskie coraz częściej postrzegają rywalizację w sferze militarnej jako ważny priorytet dla bezpieczeństwa międzynarodowego. Wnioski z analizy

strategii bezpieczeństwa Wielkiej Brytanii, Niemiec, Francji, Stanów Zjednoczonych, Chin i Federacji Rosyjskiej unaoczniają zmianę kierunków prowadzonej rywalizacji strategicznej i materializacji nowych zagrożeń. Potwierdzeniem tej tezy są działania Federacji Rosyjskiej w Syrii i na Ukrainie, nasilające się uderzenia wielu państw w cyberprzestrzeni, zjawisko masowej migracji i dążenia Chin do globalnej dominacji (National, 2016, s. 3).

Chiny posiadają ambitną strategię rozwoju globalnego, która wykorzystuje inwestycje infrastrukturalne do rozszerzenia politycznej, ekonomicznej i militarnej potęgi państwa. Wykorzystują pomoc gospodarczą do wywierania presji na zagraniczne rządy, by te przyjęły korzystną politykę w takich kwestiach jak Tajwan, Hongkong, czy chińskiej kontroli nad wyspami na Morzu Południowochińskim. Celem Jinping Xi jest stworzenie ogromnej sieci kolei, autostrad, rurociągów energetycznych, morskich szlaków handlowych i portów, które połączą Chiny z resztą Azji, Europy, Bliskim Wschodem i Afryką. Szlaki morskie mają połączyć chińskie porty morskie z państwami leżącymi na Morzu Południowochińskim, Oceanie Indyjskim, Południowym Pacyfiku i Morzu Śródziemnym (Jones, 2021, s. 3).

Stany Zjednoczone dominują w sferze militarnej, choć nie w takim stopniu jak dziesięć czy dwadzieścia lat temu. Jednak ich globalna przewaga militarna może zostać zniwelowana, jeśli Chiny lub Rosja będą w stanie wybrać korzystny fizyczny i polityczny grunt dla krótkiego i decydującego konfliktu militarnego. Wydaje się, że ani Rosja, ani Chiny nieposiadają wystarczającej siły, aby móc zwyciężyć w długotrwałym starciu militarnym ze Stanami Zjednoczonymi ani dziś, ani w przewidywalnej przyszłości (Brands, Beckley, 2021). Amerykańska dominacja militarna jest atutem w nadchodzącej erze rywalizacji wielkich mocarstw. Jednak dla skutecznego konkurowania konieczna jest poprawa zdolności związanych z wykorzystaniem niemilitarnych instrumentów oddziaływania strategicznego (Repnikova, 2022). Chiny już obecnie mają możliwości poważnego ograniczenia amerykańskiej (lub rosyjskiej) działalności wojskowej w Azji Wschodniej, na zachodnim Pacyfiku (Sullivan, Brands, 2020), a szczególnie w cyberprzestrzeni (Demchak, 2019) i coraz częściej w przestrzeni kosmicznej (Broad, 2021). Oznacza to, że Stany Zjednoczone powinny dokonać weryfikacji strategii w tych regionach i uwzględnić w niej posiadaną przewagę ideologiczną, wykorzystanie siły miękkiego oddziaływania i ograniczenia konkurencyjności chińskiej gospodarki (Lynch, 202, s. 99). Federacja Rosyjska obecnie dysponuje wyraźną przewagą militarną, gospodarczą i

informacyjną w obszarach tzw. bliskiej zagranicy i ograniczone, ale niebagatelne zdolności do projekcji siły i utrzymania wpływów na Bliskim Wschodzie (Banasik, 2021), w Arktyce oraz zdolności do prowadzenia operacji w cyberprzestrzeni (Pijović, 2021). Jednak ekonomiczne, ideologiczne i polityczne uwarunkowania Rosji oraz ewentualna przegrana wojny z Ukrainą może spowodować, że utraci te wpływy.

Nie należy z góry zakładać, że wszystkie mocarstwa chcą się angażować w spory militarne. Jednak niektóre z nich, szczególnie agresywne, dysponujące twardymi instrumentami oddziaływania międzynarodowego są skłonne do podporządkowywania sobie sąsiadów przy pomocy sił zbrojnych. Państwa takie nazywane są w literaturze rewizjonistycznymi. Tak więc niestabilności w sferze bezpieczeństwa są pochodną intencji tychże państw. Przez państwa rewizjonistyczne rozumie się zazwyczaj te, które dążą do zmiany obowiązującego *status quo* (Dobriansky, 2020). Nie kierują się brakiem bezpieczeństwa ani potrzebami jego zapewniania, ale ideologią i dominacją, co oznacza, że dążą do większej władzy (Brands, 2020). W tym sensie Federacja Rosyjska jest zdeterminowana, by zostać uznaną jako jedno z wiodących mocarstw w świecie wielobiegunowym, aby uzyskać wyższy stopień kontroli nad swoimi peryferiami i odzyskać tam autorytet niekwestionowanego hegemona (Mcclintock i inni, 2021, s. 2). Prawdopodobnie te założenia wraz z celem przetrwania reżimu stanowiły powody do inwazji na Ukrainę w lutym 2022 roku. Wydaje się więc, że Federacja Rosyjska mimo widocznej ofensywnej agresji, w swoim przekonaniu i narracji preferuje defensywne podejście do tworzonych przestrzeni rosyjskich interesów oraz rozbijania i podważania amerykańskiej hegemonii (Mazarr, 2022, s. 30). Takie podejście do rywalizacji stwarza globalne i regionalne niestabilności. Jednak oferowanie ustępstw państwu rewizjonistycznemu może po prostu przekonać je, że istniejące wpływy na rzecz wielkomocarstwowego rywala mogą nie przynieść stabilności, ale po prostu dają mu lepszą pozycję, z której będzie mógł realizować swoje kolejne ambicje. Wojna na Ukrainie potwierdza też tezę, że największe ryzyko konfliktu w systemie międzynarodowym wynika z niepowodzenia odstraszania strategicznego, a nie z błędnej percepcji zagrożeń (Ashford, 2021, s. 6).

Specyfika rywalizacji w cyberprzestrzeni

Dążenia wielkich mocarstw do uzyskania przewagi i dominacji konfrontacyjnej wykraczają daleko poza sferę bezpośredniego konfliktu zbrojnego. Operacje prowadzone w cyberprzestrzeni są chyba najbardziej oczywistym narzędziem dokonywania współczesnego podboju innych państw. Cyberprzestrzeń jest domeną, w której państwa stosując wysoko ryzykowne strategie, destabilizują środowisko bezpieczeństwa międzynarodowego (Nye, 2017, s. 15). Cyberprzestrzeń przekształciła się w coś, co stratedzy wojskowi uważają za nową przestrzeń bitewną. Nowa sfera strategicznej rywalizacji może stać się punktem wyjściowym do kolejnego globalnego wyścigu zbrojeń. Chociaż myślenie strategiczne na temat wojny w cyberprzestrzeni jest wciąż w początkowej fazie, to różne państwa utworzyły struktury dowodzenia i powołały odrębne jednostki wojskowe, posiadające techniczne kompetencje do prowadzenia ofensywnych operacji w cyberprzestrzeni (Blessing, 2021). W ciągu ostatniej dekady cyberprzestrzeń była coraz częściej wykorzystywana przez państwa do prowadzenia działań o charakterze szpiegowskim, a także działalności sabotażowej i wywrotowej (Domingo, 2016, s. 1). Dokonywano również kradzieży tajemnic przemysłowych oraz wpływano na przebieg wyborów i procesów demokratycznych w państwach Zachodu. Główne mocarstwa poszukują również sposobów do prowadzenia za pomocą środków wirtualnych destrukcyjnych form konfliktu o dużej skali bezpośrednio zagrażającym bezpieczeństwu ekonomicznemu i politycznemu (Schneider, 2016, s. 220).

Główne wyzwania związane z cyberprzestrzenią dotyczą szybkości propagacji informacji, a także sposobu, w jaki maszyny potrafią się adaptować do uwarunkowań prowadzonego konfliktu. Relacje pomiędzy oddziałującymi na siebie stronami konfliktu w czasie i przestrzeni sprowadzają się do osiągnięcia możliwości swobody działania i uzyskania kontroli nad przeciwnikiem. Taką szansę daje właśnie cyberprzestrzeń, aczkolwiek w nieco innych proporcjach jak w świecie fizycznym. Zdolności wykorzystywane w cyberprzestrzeni są kluczowymi, a nawet krytycznymi elementami oddziaływania międzynarodowego i umożliwiają osiąganie synergicznych efektów we wszystkich innych domenach operacyjnych. Należy jednak wyraźnie zaznaczyć, że uzyskanie kontroli nad przeciwnikiem w sferze wirtualnej ułatwia przejmowanie kontroli w wymiarze fizycznym, lub wpływanie na podejmowane przez niego decyzje (Crowell, 2017, s. 5).

Chiny dążąc do skompensowania przewagi militarnej Stanów Zjednoczonych, rozwijają zdolności do prowadzenia wojny w cyberprzestrzeni. Wykorzystują uzależnienie funkcjonowania amerykańskiej infrastruktury krytycznej od Internetu, stosunkowo słabą obronę cybernetyczną, a szczególnie podatność amerykańskich systemów militarnych wykorzystujących cyberprzestrzeń (Sánchez, Akyesilmen, 2021, s. 53). Chiny prowadzą szeroko zakrojone kampanie szpiegostwa cybernetycznego przeciwko rządowi USA i sektorowi prywatnemu (Goodman, 2010, s. 103, Handler, 2023). Działania wyspecjalizowanych chińskich jednostek cybernetycznych są ukierunkowane również na wywiad polityczny i wojskowy. W dłuższym czasie celem tego rodzaju kampanii jest doprowadzenie do zmanipulowania informacji, a następnie jej wykorzystanie do celu osiągnięcia przewagi politycznej, militarnej lub ekonomicznej (Sánchez, Akyesilmen, 2021, s. 55). Stany Zjednoczone koncentrują się na zapobieganiu możliwości przeprowadzenia agresywnych rosyjskich i chińskich operacji w cyberprzestrzeni, które mogłyby doprowadzić do uzyskania przewagi strategicznej (Sharpening, 2018, s. 1). Federacja Rosyjska prowadzi operacje wywiadowcze przy pomocy własnych hakerów wojskowych i podmioty zastępcze. Rosyjskie operacje w cyberprzestrzeni są coraz bardziej agresywne i mają na celu stworzenie podstaw do przyszłych poważnych zakłóceń funkcjonowania infrastruktury krytycznej atakowanych państw obejmujących między innymi sektor energetyczny, dostawy wody, funkcjonowanie lotnictwa cywilnego, obiekty handlowe i przemysłowe, a także uniemożliwienie wykorzystania zdolności militarnych. Dla przykładu zamknięty w 2017 roku przez USA konsulat Rosji w San Francisco uznawany był za węzeł wywiadowczy, służący do fizycznego mapowania sieci światłowodowych oraz szeregu innych działań uznanych za niezwykle agresywne i wysoce innowacyjne sposoby zbierania informacji wywiadowczych (Dorfman, 2017).

Federacja Rosyjska coraz częściej i skuteczniej prowadzi operacje w cyberprzestrzeni wymierzone w państwa europejskie. Jednak przywódcy tych państw niechętnie się do tego publicznie przyznają. Być może ze względu na to, że trudno jest znaleźć dowody na prowadzenie tych operacji, a być może państwa nie chcą ujawniać negatywnych konsekwencji takich działań. Rosyjskie operacje w cyberprzestrzeni szczególnie intensywnie były prowadzone przed i po rozpoczęciu wojny z Ukrainą. Można nawet pokusić się o tezę, że ze względu na wspieranie Ukrainy Zachód jest w stanie wojny w cyberprzestrzeni z Federacją

Rosyjską (Deni, 2018). Wydaje się, że obecnie większość państw europejskich jest przeciwna prowadzeniu operacji ofensywnych w odpowiedzi na ataki Rosji. Wyjątkiem jest tu Polska i Wielka Brytania skłonne do prowadzenia takich operacji (National Cyber). Być może ze względu na szkody jakie wyrządzi Federacja Rosyjska w cyberprzestrzeni innym państwom, rok 2024 może się okazać przełomowy i doprowadzi do zmiany ich decyzji co do prowadzenia operacji o charakterze ofensywnym przeciwko agresorowi, aby nie pozostawać biernym i nie tworzyć wrażenia jego bezkarności.

Coraz częściej pojawiają się głosy, że w cyberprzestrzeni powinno być prowadzone odstraszanie strategiczne na wzór konwencjonalnego, zakotwiczonego w strategicznej przestrzeni konfliktu zbrojnego. Ze względu jednak na pewną specyfikę funkcjonowania cyberprzestrzeni można postawić tezę, że aktualnie rywalizacja jest prowadzona głównie w szarej strefie. Praktyka operacyjna potwierdza, że odstraszanie w cyberprzestrzeni nie działa, a główne mocarstwa zadają i przyjmują niedozwolone prawem ciosy. Zrozumienie dynamiki interakcji, jaką wywołuje ta aktywna strategia rywalizacji jest kluczowe, zwłaszcza biorąc pod uwagę obawy niektórych decydentów, że aktywna postawa USA w cyberprzestrzeni może doprowadzić do niekontrolowanej eskalacji konfliktów. Z wypowiedzi niektórych amerykańskich ekspertów wynika, że w cyberprzestrzeni mogą mieć miejsce najbardziej spiralne i niekontrolowane rodzaje konfliktów, z jakimi kiedykolwiek mieliśmy do czynienia (Committee, 2017, s. 7).

Stosowane w ramach rywalizacji strategicznej odstraszanie nie jest ograniczone do przestrzeni konfliktu zbrojnego. Skoro eskalacja ma miejsce w cyberprzestrzeni to pojawia się problem zarządzania tego typu konfliktem. Warto również zastanowić się nad tym, w jaki sposób rywale strategiczni będą poszukiwać możliwości osiągania przewagi strategicznej w tej przestrzeni i jak ich skutecznie odstraszać od tego typu działań, szczególnie wtedy, gdy nie będzie prowadzony konflikt zbrojny w świecie rzeczywistym. Zachowania w cyberprzestrzeni, które nie są związane z konfliktem zbrojnym, nie muszą być skoncentrowane na poszukiwaniu przewagi militarnej, ale mogą dotyczyć wybranych domen rywalizacji strategicznej (Fischerkeller, Harknett, 2019).

Istnieją strukturalne czynniki zniechęcające do eskalacji zagrożeń w przestrzeni cybernetycznej, w przypadku, gdy nie ma rzeczywistego konfliktu zbrojnego. Ze względu na wzajemne powiązania, które są podstawową cechą strukturalną cyberprzestrzeni, cele strategiczne można osiągać w, poprzez i przy pomocy cyberprzestrzeni, za

pośrednictwem operacji lub kampanii cybernetycznych, które nie muszą wcale być związane z konfliktem zbrojnym. Podstawowym warunkiem wynikającym z wzajemnych powiązań jest stały kontakt z rywalem, co w połączeniu z charakterem technologii informacyjnych i sieciowych systemów komputerowych narzuca strukturalny imperatyw bezpieczeństwa zakładający, że przeciwnicy mogą ciągle się angażować w prowadzenie tego typu operacji. Pojawia się zatem perspektywa osiągnięcia strategicznych korzyści, polegających na pozyskaniu nowych źródeł siły narodowej, poprzez występowanie skumulowanych efektów możliwych do osiągania dzięki dobrze zorganizowanym kampaniom prowadzonym w cyberprzestrzeni (Fischerkeller, Harknett, 2019).

Zakończenie

Współczesne środowisko strategiczne charakteryzuje się ciągłą, globalną rywalizacją, zarówno powyżej, jak i poniżej progu konfliktu zbrojnego. Rywalizacja strategiczna może się materializować w wielu formach. Różne państwa mogą rywalizować na różne sposoby, a hierarchia celów zmienia się w czasie. Stosownie do tego dobierane są zdolności i sposoby ich zastosowania w celu wywoływania efektów strategicznych, których suma ma doprowadzić do oczekiwanych rezultatów politycznych. Dla utrzymania stabilności bezpieczeństwa międzynarodowego kluczowa jest strategiczna ocena środowiska oraz zidentyfikowanie rodzaju, zakresu i intensywności rywalizacji, z którą przyjdzie się zmierzyć w przyszłości przez pojedyncze państwo, lub koalicję państw. Rywalizacja strategiczna polega na próbie zdobycia przewagi w stosunku do innych. Może być rozumiana jako egoistyczna pogoń za władzą, bogactwem, wpływami i statusem, co niesie za sobą określone wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego. Rywalizacja nie jest synonimem konfliktu. Jest ciągłym procesem dotyczącym interakcji nie tylko międzypaństwowych, ale również aktorów niepaństwowych i podmiotów indywidualnych. Na jednym końcu tych interakcji mamy do czynienia ze współpracą, a na drugim z konfrontacją. Państwa współpracujące są wyjątkowo zgodne co do celów politycznych i środków do ich osiągnięcia, dzięki czemu mogą harmonijnie je osiągać. Państwa ze sobą rywalizujące charakteryzują się skrajnie przeciwstawnymi celami, które mogą stanowić zagrożenia, a dominująca forma interakcji pomiędzy państwami przekształca się w konflikt zbrojny.

Wnioski z badań upoważniają do stwierdzenia, że podstawowe interesy narodowe i ambicje państw rewizjonistycznych, w tym

Federacji Rosyjskiej, a także podstawowe czynniki wpływające na charakter rywalizacji pozostają niezmienne. Nie można jednak przypuszczać, że amplituda intensywności rywalizacji w przyszłości się zmniejszy. Potencjał dalszej eskalacji konfliktów jest bardzo wysoki. Świadczą o tym coraz głębsze podziały, występujące pomiędzy Stanami Zjednoczonymi a Chinami zarysowujące się na gruncie zarówno wojny na Ukrainie, jak i wokół statusu Tajwanu. Chiny, dysponując mocną gospodarką, ambitnymi planami globalnymi i agresywnymi zamiarami regionalnym będą dążyły do uzyskania globalnej przewagi. Słaba gospodarka Federacji Rosyjskiej nie pozwoli na zmianę globalnego systemu bezpieczeństwa bez agresywnego użycia siły militarnej, dlatego też przyszłe bezpieczeństwo będzie ściśle uzależnione od form i zakresu rywalizacji prowadzonej pomiędzy Chinami a Stanami Zjednoczonymi. Może ona przybrać formę bezpośredniego starcia o wpływy regionalne, walkę o przewagę ekonomiczną i ideologiczną, lub inną, bardziej łagodną formę dążenia do osiągania własnych celów politycznych.

Na podstawie przeprowadzonych badań ustalono, że wraz z rozwojem technologii zmienia się charakter rywalizacji i generowanych zagrożeń. Zmianie ulegają strategie prowadzenia wojen, a także koncepcje operacyjne i techniki wsparcia związane z tymi zmianami. Stale wzrastająca rola i znaczenie cyberprzestrzeni stwarza nowe uwarunkowania do prowadzenia rywalizacji strategicznej i jednocześnie staje się główną przestrzenią, w której jest podejmowana walka. Cyberprzestrzeń jest najnowszą domeną operacyjną i przestrzenią, w której będzie przebiegała przyszła rywalizacja oraz kluczowym integratorem wszystkich innych domen i operujących w nich zdolności. Otworzyła nowy wymiar polityki siły, w którym kampanie cybernetyczne stają się kluczowe dla osiągania przewagi strategicznej oraz celów strategicznych bez uciekania się do konwencjonalnych działań zbrojnych.

Prowadzenie operacji w cyberprzestrzeni ma i będzie miało decydujące znaczenie dla osiąganych efektów zarówno w świecie rzeczywistym, jak i wirtualnym, co podkreśla znaczenie szeroko rozumianej sfery informacyjnej. Cyberprzestrzeń z jednej strony jest integratorem innych domen, a z drugiej strony jest środowiskiem, w którym prowadzona jest rywalizacja. W cyberprzestrzeni może być prowadzone odstraszanie i wymuszanie oraz można osiągać znaczne efekty kinetyczne i niekinetyczne o znaczeniu politycznym. Cyberprzestrzeń staje się polem bitwy toczonej wspólnie lub w oderwaniu od innych, konwencjonalnych środków walki.

Dzięki cyberprzestrzeni możliwe jest zjawisko konwergencji powstające w rezultacie harmonizowania wszystkich dostępnych zdolności. Pozwala to na stosowanie wielorakich form atakowania przeciwnika, przejmowanie nad nim inicjatywy i w końcu narzucanie mu własnej woli. Dzięki temu możliwe jest też optymalizowanie efektów osiąganych w wymiarze fizycznym, wirtualnym i poznawczym, a ich agregacja sprzyja pokonaniu rywala strategicznego. Powstającą synergię międzydomenową można uznać za ewolucyjną formę manewru broni połączonej. Dzięki cyberprzestrzeni możliwe jest też prowadzenie rywalizacji poniżej konfliktu zbrojnego oraz koncentrowanie się na najbardziej podatnych na oddziaływanie zdolnościach rywala strategicznego. Prowadzi to wniosku, że obecnie cyberprzestrzeń stanowi nie tylko główny filar prowadzenia rywalizacji strategicznej, ale jest również jej alternatywą.

Literatura

Air Force Doctrine Publication, 2023. *Cyberspace Operations*, Waszyngton.

Ashford, E., 2021. *Revisionist States are the Cause of Great-Power Competition*, Atlantic Council 04.02. 2021.

Bagińska, J., 2018. *Bezpieczeństwo infrastruktury krytycznej sektora ropy naftowej w aspekcie zagrożeń hybrydowych*, Warszawa.

Banasik, M., 2021. *Rywalizacja, presja i agresja Federacji Rosyjskiej. Konsekwencje dla bezpieczeństwa międzynarodowego*, Warszawa.

Bennett, D.S., 1996. *Security, Bargaining, and the End of Interstate Rivalry,* International Studies Quarterly, Vol. 40, No. 2, s. 157–183.

Białoskórski, R., 2023. *Geopolitics of the information age,* Przegląd Geopolityczny, 46, s. 155-165.

Blessing, J., 2021. *The Global Spread of Cyber Forces, 2000–2018*, 13th International Conference on Cyber Conflict, Tallin.

Bógdał-Brzezińska, A., 2023. *Effectiveness od Russia's cyberaggression against Ukraine in 2022/2023*, Przegląd Geopolityczny, 44, s. 25-40.

Brands, H., 2020. *Don't Let Great Powers Carve Up the World,* Foreign Affairs 26.04.2020, https://www.foreignaffairs.com/articles/china/2020-04-20/dont-letgreat-powers-carve-world, dostęp 09.11.2023.

Brands, H., Beckley, M., 2021. *China Is a Declining Power—and That's the Problem*, Foreign Policy 24.10.2021,

https://foreignpolicy.com/2021/09/24/china-great-power-united-states/, dostęp 02.10.2023.

Broad, W.J., 2021. *How Space Became the Next 'Great Power' Contest Between the U.S. and China*, The New York Times 21.02.2021, https://www.nytimes.com/2021/01/24/us/politics/trump-biden-pentagon-space-missiles-satellite.html, dostęp 28.010.2023.

Burkhart, D., Woody, A., 2017. *Strategic Competition Beyond Peace and War*, 20 Forum/Strategic Competition: Beyond Peace and War JFQ 86, 3rd Quarter 2017, s. 20-27.

Committee on Armed Services House of Representatives, 2017. *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities*, Waszyngton.

Crowell, R.M., 2017. *Some Principles of Cyber Warfare Using Corbett to Understand War in the Early Twenty–First Century,* London.

Deconstructing US-China Competition, 2021. TI Observer, Vol. 09, s. 1- 45.

Demchak, C.C., 2019. *China: Determined to dominate cyberspace and AI*, Bulletin of the Atomic Scientists Volume 75, 2019 - Issue 3, s. 99-104.

Deni, J.R., 2018. *The West's Confusion over Russia's Cyberwars*, Carnegie Europe 08.03.2018, https://carnegieeurope.eu/strategiceurope/75740, dostęp 24.10.2023.

Dobriansky, P., 2020. *Ask the Experts: Should US Foreign Policy Focus on Great-Power Competition?*, Foreign Affairs 14.10.2020, https://www.foreignaffairs.com/ask-the-experts/2020-10-13/should-us-foreign-policy-focus-great-power-competition, dostęp: 24.10.2023.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, 2015, Warszawa.

Domingo, F.C., 2016. *Conquering a new domain: Explaining great power competition in cyberspace*, Comparative Strategy 2016, 35, 2, s. 154–168.

Dorfman, Z., 2017. *The Secret History of the Russian Consulate in San Francisco*, Foreign Policy 14.12.2017, https://foreignpolicy.com/2017/12/14/the-secret-history-of-the-russian-consulate-in-san-francisco-putin-trump-spies-moscow/, dostęp 24.10.2023.

Dubisz, S., (red.), 2006. *Uniwersalny słownik języka polskiego*, Warszawa.

Evans, A.T., 2023. *Alternative Futures Following a Great Power War, Volume 2.* Supporting Material on Historical Great Power Wars, Santa Monica.

Fischerkeller, M.P., Harknett, R.J., 2019. *What is Agreed Competition in Cyberspace?*, Lawfare 19.02.2019, https://www.lawfareblog.com/what-agreed-competition-cyberspace, dostęp 24.10.2023.

Framework For Future Alliance Operations, 2018. North Atlantic Treaty Organisation, Bruksela.

Friis, K., Ringsmose, J., 2016. *Conflict in Cyber Space Theoretical, Strategic and Legal Pespectives*, Routledge 2016.

Goodman, W., 2010. *Cyber Deterrence. Tougher in Theory than in Practice?*, Strategic Studies Quarterly, Fall 2010, s. 102-135.

Gomez, M.A., 2023. *Tracing Strategic Preferences in Cyberspace: The Role of Regional and Domestic Strategic Culture,* Comparative Strategy, Volume 42, 2023, s. 103-127.

Gürer, C., 2021. *Strategic Competition: International Order and Transnational Organized Crime*, The George C. Marshall European Center for Security Studies, https://www.marshallcenter.org/en/publications/security-insights/strategic-competition-international-order-and-transnational-organized-crime-0#toc-strategic-competition-hard-and-soft-security-issues-, dostęp 13.10.2023.

Handler, S., 2023. *The 5×5—China's Cyber Operations*, Atlantic Council.

Harknett, R.J., Smeets, M., 2020. *Cyber Campaigns and Strategic Outcomes*, Journal of Strategic Studies 45, 3, 1-34.

Hensel, P.R., 1999. *An Evolutionary Approach to the Study of Interstate Rivalry*, Conflict Management and Peace Science, 17, 2, s. 1-34.

Hoffman, F., 2016. *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War*, The Heritage Foundation, s. 25-36.

Joine, K.F., Tutty, M.G., 2018. *A Tale Of Two Allied Defence Departments: New Assurance Initiatives for Managing Increasing System Complexity, Interconnectedness, and Vulnerability*, Australian Journal of Multi-Disciplinary Engineering, 14, 1, s. 4-25.

Jones, S.G., 2021. *Hiding and Finding The Challenge of Security Competition*, CSIS Brief, s. 1-13.

Kamińska-Szmaj, I., (red.), 2001. *Słownik wyrazów obcych*, Wrocław.

Kapusta, P., 2015. *The Gray Zone*, Special Warfare, 28, 4.

Klein, J.P., Goertz, G., Diehl, P.F., 2006. *The New Rivalry Dataset: Procedures and Patterns,* Journal of Peace Research, 43, 3, s. 331–348.

Kosenkov, A., 2016. *Cyber Conflicts as a New Global Threat*, Future Internet, 8, 3.

Kuusisto, T., Kuusisto, R., 2015. *Cyber World as a Social System*, Chapter from book Specialized Honeypots for SCADA Systems, Springer.

Lynch, T.F., 2020. *Strategic Assessment 2020. Into a New Era of Great Power Competition,* Waszyngton 2020.

Marczyk, M., 2018. *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, Przegląd Teleinformatyczny, 1-2.

Mazarr, M.J., 2022. *Understanding Competition. Great Power Rivalry in a Changing International Order—Concepts and Theories*, Santa Monica.

Mazarr, M.J., 2021. *Stabilizing Great-Power Rivalries*, Santa Monica.

Mazarr, M.J., Blake, J., Casey, Mcdonald, A, T., Pezard, S., Spirta, M., 2018. *Understanding the Emerging Era of International Competition*, Santa Monica.

Mcclintock, B., Hornung, J.W., Costello, K., 2021. *Russia's Global Interests and Actions. Growing Reach to Match Rejuvenated Capabilities*, Santa Monica.

Milner, H., 1992. *International Theories of Cooperation: Strengths and Weaknesses*, World Politics, 44, 3, s. 466-496.

Modrzejewski, Z., Dejnacki, M., 2023. *Walka informacyjna w rosyjskiej kulturze strategicznej*, Przegląd Geopolityczny, 46, s. 104-118.

Mundt, P., Oh, I., 2019. *Asymmetric competition, risk, and return distribution*, Economics Letters, 179, s. 29-32.

National Cyber Security Strategy 2016-2021, 2016. Londyn (in:) *National Security Strategy and Strategic Defence and Security Review 2015*, Londyn.

NATO 2022 Strategic Concept, 2022. Bruksela.

Nye, J.S., 2017. *Normative Restraints on Cyber Conflict*, Cambridge.

Olagbemiro, A.O., 2014. *Cyberspace as a Complex Adaptive System and The Policy and Opertional Implications for Cyber Warfare*, Kansas.

Pia, E., Die, T., 2006. *Conflict and Human Rights: A Theoretical Framework*, SHUR Working Paper Series, Birmingham.

Pijović, N., 2021. *The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms*, Tallin.

Raska, M., 2020. *Strategic Competition for Emerging Military Technologies. Comparative Paths and Patterns*, PRISM 8, 3.

Repnikova, M., 2022. *The Balance of Soft Power*, Foreign Affairs 22.06.2022, https://www.almendron.com/tribuna/the-balance-of-soft-power/, dostęp 13.10.2023.

Sánchez, K.V., Akyesilmen, N., 2021. *Competition for High Politics in Cyberspace: Technological Conflicts Between China and the USA*, Polish Political Science Yearbook, 50, 1, s. 43–69.

Satkiewicz, H., 1994. *Normy polszczyzny ogólnej a języki subkultur*, [w:] *Język a kultura*, t. 10: *Języki subkultur*, Wrocław, s. 9-17.

Shea, J., 2018. *Cyberspace as a Domain of Operations. What is NATO's Vision and Strategy?* MCU Journal, 9, 2, s. 133-150.

Schneider, J., 2020. *A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem*, Washington Quarterly, 43, 2, s. 160–164.

SIPRI Yearbook 2022, 2022. Stockholm International Peace Research Institute.

Soon-Kun, O., 2013. *Understanding Contemporary Interstate Rivalries: Consensus Rivalries and Rivalry Termination*, Strategy 21, 16, 2, s. 222-270.

Sullivan, J., Brands, H., 2020. *China Has Two Paths to Global Domination*, Waszyngton.

Święcicka, M., 2014. *Kilka uwag lingwisty o kontestacji*, https://repozytorium.ukw.edu.pl/bitstream/handle/item/6019/Kilka%20uwag%20lingwisty%20o%20kontestacji.pdf?sequence=1&isAllowed=y, dostęp: 13.10.2023.

The Concept of Potential Competition, 2021. OECD Competition Committee Discussion Paper, https://www.oecd.org/daf/competition/the-concept-of-potential-competition-2021.pdf, dostęp 13.10.2023.

U.S. Department of Defense, 2018. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Waszyngton.

Vasquez, J .A., 1996. *Distinguishing Rivals That Go to War from Those That Do Not: A Quantitative Comparative Case Study of the Two Paths to War*, International Studies Quarterly, 40, 531-558.

White House, 2017. *National Security Strategy of the United States of America*, Waszyngton.

Banasik, M., Chojnowski, L., 2024. *Rywalizacja strategiczna w cyberprzestrzeni i jej konsekwencje dla bezpieczeństwa międzynarodowego,* Przegląd Geopolityczny, 48, s. 69-90.

Streszczenie:

Celem badań było wyjaśnienie mechanizmów prowadzenia rywalizacji strategicznej, w tym w cyberprzestrzeni oraz zidentyfikowanie wyzwań i zagrożeń z niej wynikających dla bezpieczeństwa międzynarodowego. Do rozwiązania problemów badawczych zastosowano analizę i krytykę literatury, obserwację nieuczestniczącą oraz studium przypadków. W procesie badawczym ustalono, że w najbliższej dekadzie rywalizacja strategiczna będzie najbardziej intensywnie przebiegała pomiędzy Stanami Zjednoczonymi, a Chinami i Federacją Rosyjską. Największymi zagrożeniami dla obowiązującego ładu międzynarodowego będą ambicje państw rewizjonistycznych związane z roszczeniami terytorialnymi i rozszerzaniem stref wpływów. Państwa te będą wykorzystywać głównie niemilitarne instrumenty oddziaływania, w tym cyberprzestrzeń, aby uzyskać przewagę nad konkurującymi ze sobą społeczeństwami. Cyberprzestrzeń stanowić będzie nie tylko główny filar rywalizacji, ale również dla niej alternatywę.

Słowa kluczowe: rywalizacja strategiczna, bezpieczeństwo międzynarodowe, cyberprzestrzeń, Chiny, Stany Zjednoczone, Federacja Rosyjska, wyzwania i zagrożenia.