Chiny, 5G i bezpieczeństwo sojuszu po szczytach NATO w 2021/22 rokuw świetle ataku na Ukrainę

Tekst prezentuje kluczowe wnioski wyciągnięte z obrad okrągłego stołu, zorganizowanego przez GMF i przeprowadzonego według zasady Chatham House. Spotkanie zgromadziło ekspertów z Europy i Stanów Zjednoczonych w celu zbadania w jaki sposób szeroko rozumiana problematyka Chin, sieci 5G, odporności i infrastruktury krytycznej jest adresowana w kontekście NATO. Obrady okrągłego stołu zostały przeprowadzone w 2021 roku, lecz zarówno jego wnioski, jak i analiza, zostały uaktualnione po rosyjskiej inwazji na Ukrainę i szczycie NATO w Madrycie w 2022 roku.

- Inwazja Rosji na Ukrainę pokazała wyraźnie, jak niezbędna jest rola NATO, jeśli chodzi o zapewnianie bezpieczeństwa europejskim sojusznikom. Z kolei ogłoszona przez Chiny „nieograniczona" współpraca z Rosją świadczy o tym, że spektrum zagrożeń, z jakimi sojusz musi się teraz liczyć, jest znacznie szersze. Potwierdza to konieczność dopilnowania, aby pakt przystosował się odpowiednio do wszystkich wymiarów, z jakimi musi się mierzyć w nowym pod względem bezpieczeństwa środowisku.
- Biorąc pod uwagę najważniejsze problemy poruszane podczas szczytu towarzyszącego wizycie prezydenta Joe Bidena w Europie latem 2021 r., jasne stało się , że przez wiele kolejnych lat Chiny pełnić będą centralną rolę w zakresie stosunków transatlantyckich. Kraj ten krzyżuje się obecnie na wielu płaszczyznach z programem NATO, zajmując teraz jeszcze bardziej ugruntowane miejsce w dyskusji, niż to było do tej pory. Wprawdzie NATO nie prowadzi konfliktu zbrojnego z Chinami, jednak państwo to jest kluczowym rywalem geopolitycznym dla całego Zachodu. Co więcej Stany Zjednoczone postrzegają je jako główne źródło zagrożenia dla bezpieczeństwa krajowego i istnieje kilka potencjalnych opcji, kiedy obie strony mogą zostać wciągnięte w konfrontację militarną. Pomimo tego że Europa jest podzielona w tej sprawie, sojusznicy europejscy tradycyjnie akceptują część programu dotyczącego bezpieczeństwa i obrony USA w zamian za gwarancje bezpieczeństwa. Chiny stanowią jednak również źródło zagrożeń, które dotyczą w sposób konkretny bezpieczeństwa krajów Starego Kontynentu. Szczególnym problemem jest kwestia odporności i infrastruktury krytycznej, biorąc pod uwagę znaczne uzależnienie się Europy od chińskiej technologii w zakresie infrastruktury cyfrowej. Aktualna debata dotyczy tego, czy NATO jest najwłaściwszą platformą, na której należy rozwiązywać tego typu problemy, czy może bardziej aktywną rolę powinna tutaj pełnić Unia Europejska, albo czy można podzielić obowiązki w tym zakresie pomiędzy te dwie organizacje.
- Sektor telekomunikacji został zidentyfikowany przez NATO jako nowy obszar zainteresowania. Aby móc realizować swoje kluczowe zadanie polegające na wspólnej polityce obronnej, konieczna jest bardziej odporna infrastruktura, która będzie w stanie poradzić sobie z atakami hybrydowymi. W większości europejskich krajów znajduje się ona jednak zazwyczaj w rękach prywatnych.Może być przez to bardziej podatna na wpływy z zewnątrz oraz skutkować również podejmowaniem decyzji gospodarczych, które mogą lekceważyć aspekty związane z bezpieczeństwem krajowym, jeśli nie zostanie to uregulowane przepisami prawa. Przykładem kraju, który stosuje różnego rodzaju taktyki hybrydowe na terytorium NATO jest Rosja. Niemniej jednak Chiny również zaczęły stosować rozmaite, skomplikowane zagrywki polityczne i niemilitarne w ramach konfrontacji z NATO na płaszczyźnie ogólnej oraz w kontaktach z indywidualnymi krajami, chcąc w ten sposób wywierać na nie polityczny i gospodarczy wpływ.
- Aby kwestia odporności mogła przyczynić się do bliższej współpracy między sojuszem północnoatlantyckim a UE, konieczne jest znalezienie równowagi, w której sprecyzowane zostaną wyraźne zadania należące do tych obu organizacji. Obecnie NATO wprowadza

program oparty na wzmacnianiu odporności, w tym w wymiarze niemilitarnym. Sojusz koncentruje się głównie na koordynacji i konsultacjach na płaszczyźnie politycznej, zarządzaniu kryzysowym oraz wspólnych działaniach obronnych, a także na interoperacyjności. Z drugiej strony Unia ma do dyspozycji szereg instrumentów regulacyjnych, począwszy od zestawu narzędzi dotyczących bezpieczeństwa sieci 5G, a kończąc na Europejskim planie działania na rzecz demokracji, w którym poruszono niektóre z szerszych problemów dotyczących odporności. Z uwagi na to konieczne jest ustalenie wspólnej płaszczyzny współpracy i obowiązków w relacjach EU i NATO. Trzeba również rozważać tradycyjne planowanie zdolności militarnych w kontekście wymagań związanych z odpornością, ponieważ będzie to jeden z kluczowych filarów przyszłej współpracy w relacjach sojuszu z Unią Europejską.

- Nie jest jednoznaczne czy ochrona infrastruktury cywilnej leży w zakresie kompetencji sojuszu. Innymi słowy, chodzi o to, czy atak cybernetyczny na infrastrukturę cywilną w Europie spowoduje uruchomienie artykułu piątego. Jeśli nie, to czy będzie to należało do kompetencji UE? Co więcej granice dotyczące infrastruktury cywilnej i wojskowej są rozmyte, zwłaszcza jeśli chodzi o sektor telekomunikacji.

- Branża ta ma coraz większe znaczenie w zakresie funkcjonowania społeczno-gospodarczego. Jest także podstawą i przyszłością innowacji. Te dwa wymiary wiążą się z kolei z wyścigiem technologicznym. To właśnie technologia jest i będzie kluczowym elementem w zakresie zapobiegania i obrony. Przewaga technologiczna gwarantuje nie tylko wyższość na polu walki, ale również dominującą pozycję na pozostałych obszarach. Jest ona jednak uzależniona od solidnych podstaw przemysłowych podlegających ciągłemu ulepszaniu, które łączą w sobie innowacje na płaszczyźnie cywilnej i wojskowej, a także działania badawczo-rozwojowe. Konieczne są wspólne inicjatywy w zakresie innowacji łączące partnerów z obu stron Atlantyku, aby zachować i rozwijać krytyczne możliwości w odniesieniu do działań toczących się na polu walki i poza nim. W tym celu potrzebne są lepsze i skuteczniejsze związki między sektorem wojskowym i cywilnym. NATO musi znaleźć lepsze sposoby na zintegrowanie wymiaru gospodarczego, który stanowi podstawę elementów polityki bezpieczeństwa tej organizacji, zwłaszcza że strategia przemysłowa znowu znalazła się na pierwszym miejscu agendy UE i USA. Trzeba stworzyć nowe kanały polityczne, aby móc ułatwiać tego typu integrację, wzmacniając w ten sposób odporność członków sojuszu i utrzymując ich przewagę konkurencyjną.

- Obecnie wydaje się, że NATO ma problem z realizacją tego zadania. Trzeba zatem precyzyjnie zidentyfikować i sklasyfikować kwestie, które wynikają z ich kompetencji. Pierwszym krokiem, jaki powinni wykonać politycy, jest wprowadzenie jasnych parametrów w obszarach, w których współpraca gospodarcza z Chinami nie będzie miała negatywnego wpływu na bezpieczeństwo krajowe. Sojusz północnoatlantycki jest również naturalną platformą, w ramach której można dokonywać wymiany informacji dotyczących bezpieczeństwa z różnymi instytucjami, podmiotami niepaństwowymi oraz partnerami NATO, którzy posiadają doświadczenie w kontaktach z Chinami, takimi jak Japonia i Korea Południowa. W związku z tym musi dalej traktować infrastrukturę cyfrową (5G, kable podmorskie itd.) oraz Chiny ze szczególną uwagą, utrzymując.

- Biorąc pod uwagę fakt, że zagrożenia cybernetyczne stanowią od dawna obszar zainteresowania NATO, naturalne jest to, że elementem obrad członków sojuszu stała się również sieć 5G – pomimo tego że jej wymiar obronny wprowadzony został do programu z pewną zwłoką. Ponadto nie można pozwolić na to, by pominięty został kluczowy obszar związany z bezpieczeństwem, a mianowicie sposób przetwarzania i przechowywania danych. Najważniejsze problemy obejmują ochronę sektora publicznego i przemysłu, a także dopilnowanie, aby firmy, obywatele i instytucje rządowe mogli przesyłać dane do sieci w całości nieobsługiwanej przez Chiński sprzęt . Przykładowo w przypadku sieci 5G znaczącą rolę odgrywać będzie infrastruktura w chmurze. Zgodnie z przepisami obowiązującymi w Chinach, rząd tego kraju ma prawo zażądać, aby udzielono mu dostępu do danych dowolnej firmy prywatnej w Chinach, co stanowi zagrożenie w odniesieniu do wszystkich danych przechowywanych w chińskiej sieci w chmurze. Weźmy na przykład Belgię – cała infrastruktura telekomunikacyjna w tym kraju była wcześniej oparta na sprzęcie pochodzącym z Chin. Dotyczyło to również komunikacji mobilnej, z jakiej

korzystano w administracji UE i NATO. Chiński sprzęt przeniknął również do sieci niemieckich, co oznacza, że komunikacja mobilna wszystkich żołnierzy NATO stacjonujących w Niemczech odbywa się na jakimś etapie z udziałem sieci opartej na chińskiej technologii. W nowych niemieckich przepisach dotyczących bezpieczeństwa IT słusznie wspomniano o potrzebach NATO związanych z bezpieczeństwem, jeśli chodzi o ocenę wiarygodności dostawców. Widać jednak również, że aspiracje mogą znacznie odbiegać od praktyki: od czasu, gdy nowe przepisy weszły w życie, udział firmy Huawei w sieci 5G należącej do Deutsch Telekom (DT) wzrósł do ponad 60%. W 2020 r. kluczowym klientem usług w chmurze DT – stworzonej i obsługiwanej przez firmę Huawei – była Europejska Organizacja Badań Jądrowych w Szwajcarii (CERN). Innymi słowy najważniejsza instytucja prowadząca badania jądrowe przechowuje swoje dane w chińskiej chmurze. W ramach planu minimum konieczne jest zatem to, aby sieci, które pełnią jakąś rolę w sieciach rządowych, przemyśle obronnym oraz bezpieczeństwie wewnętrznym, nie były uzależnione od sprzętu pochodzącego z Chin. Co więcej sieci pełniące funkcje o znaczeniu krytycznym dla społeczeństwa, np. w sektorze mediów użytkowych, farmaceutycznym, opieki zdrowotnej, bankowości, transportu i komunikacji, również nie mogą być narażone na zagrożenia wynikające z tego powodu.

- Członkowie sojuszu z regionu Europy Wschodniej do tej pory z ostrożnością podchodzili do rosnących obaw ze strony NATO dotyczących Chin. Ich niepokój wzbudzał fakt, że w ten sposób niesłusznie odwrócona zostanie uwaga od zagrożenia ze strony Rosji. Ostatnie kilka tygodni pokazało, że NATO musi podjąć działania w zakresie obu tych problemów i poradzić sobie z zagrożeniami ze strony Rosji oraz Chin, ponieważ de facto są one ze sobą powiązane. Wojna na Ukrainie potwierdziła w sposób drastyczny bezpośrednie niebezpieczeństwo związane z agresją ze strony rosyjskiego reżimu. Z drugiej strony coraz bliższe więzi łączące Chiny z Rosją, ich otwarte poparcie dla stanowiska Rosji wobec NATO, przyjęcie przez kanały propagandowe tego kraju postawy w pełni popierającej stanowisko Moskwy oraz potencjalne zagrożenie związane z faktem, że Pekin może pospieszyć z pomocą gospodarczą dla Rosji – albo nawet transferem broni, świadczą o tym, że „nieograniczona" współpraca w stosunkach chińsko-rosyjskich stanowi w gruncie rzeczy współpracę skierowaną przeciwko Zachodowi. NATO musi wziąć pod uwagę fakt, że wspólne siły tych obu krajów mogą zostać wykorzystane w celu realizacji zarówno rosyjskich planów w Europie, jak i chińskich w Azji, a także ich wspólnych interesów w innych rejonach świata.

- Prowadzi to tym samym do drastycznego wzrostu ryzyka związanego z bezpieczeństwem ze strony chińskiego sprzętu telekomunikacyjnego wykorzystywanego w sieciach krajów Europy Środkowo-Wschodniej należących do NATO. Podczas gdy NATO zwiększa możliwości obronne na wschodniej flance w obliczu zagrożenia ze strony Rosji, sieci telekomunikacyjne w Polsce, Rumunii i innych krajach w dalszym ciągu uzależnione są w dużym stopniu od sprzętu pochodzącego z Chin. Tak naprawdę żadne z tych państw nie zadbało o to, aby w kolejnych latach wyeliminować ze swojego rynku niewiarygodnych dostawców. Jak dotąd najbardziej rygorystyczne przepisy mówią o tym, by ograniczyć wprowadzanie nowego chińskiego sprzętu, jednak akceptują ryzyko związane ze stosowaniem niewiarygodnego starego sprzętu do połowy obecnej dekady a nawet dłużej. Takie podejście jest niedopuszczalne. Groźba, że w przypadku konfliktu Chiny udzielą Rosji dostępu np. do polskich sieci telekomunikacyjnych za pośrednictwem firm Huawei lub ZTE, jest realna i może się wiązać z dramatycznymi konsekwencjami.

- Koszt wymiany chińskiej infrastruktury w Europie nie powinien stanowić tutaj ograniczenia: w miarę przechodzenia z technologii 4G do 5G operatorzy zmuszeni będą i tak do wymiany istniejącego sprzętu na nowy. Tym samym całkowity zakaz korzystania z nowego sprzętu firmy Huawei może zostać zrealizowany w sposób „naturalny" w ciągu około sześciu lat, po czym zainstalowana, niewiarygodna baza zostanie po prostu wycofana. Problemem jest raczej to, by zdecydować się na szybsze przejście w kierunku wiarygodnych technologii z uwagi na potrzeby związane z bezpieczeństwem krajowym, gdzie krótkoterminowe względy handlowe dotyczące terminu wycofywania sprzętu nie powinny wpływać na tempo wprowadzania tych zmian. Kolejnym powracającym mitem jest to, że chińscy dostawcy są bardziej zaawansowani technologicznie od ich europejskich odpowiedników. Stany Zjednoczone oraz Korea Południowa, które zajmują czołowe miejsca pod względem wprowadzania sieci 5G, korzystają z infrastruktury wolnej w całości od

sprzętu pochodzącego z Chin, opierając się w większości na technologii europejskiej. Jeśli chodzi o ceny, dostawcy z Europy również są w stanie konkurować ze swoimi chińskimi rywalami, nie są jednak w stanie konkurować z chińskim państwem. Stosowanie w tym kraju dopłat rządowych do rodzimych firm prowadzących działania na rynku globalnym a także faworyzowanie chińskich podmiotów na rynku krajowym prowadzi do dalszych wypaczeń w zakresie równości szans. Problem ten dotyczy w największym stopniu niewielkich operatorów z Europy, Ameryki Łacińskiej i Azji, którzy mają mniejsze możliwości kredytowe, dlatego muszą się decydować na pożyczki oferowane przez Chińczyków ze względu na brak alternatywnych mechanizmów w zakresie finansowania. Jednym z proponowanych rozwiązań alternatywnych jest tutaj Open-RAN. W praktyce jednak obecność Chińczyków i ich wpływ w zakresie struktur rozwojowych musi budzić wątpliwości i wiąże się z koniecznością przeprowadzenia kompleksowej oceny ryzyka.

- Dobrym punktem wyjścia, jeśli chodzi o dalsze działania, jest zestaw narzędzi dotyczących bezpieczeństwa sieci 5G UE. Jednakże ze względu na fakt, że ma on charakter nieobowiązkowy, może być różnie interpretowany i wdrażany przez państwa członkowskie, co prowadzi tym samym do pojawienia się słabych punktów. Jednym z konkretnych dalszych kroków może być dopilnowanie, aby narzędzia te wdrożone zostały we wszystkich krajach Unii w sposób bardziej rygorystyczny. Niemniej jednak zestaw ten stanowi jedynie punkt wyjścia. Sieci transmisyjne, światłowody łączące zasoby krytyczne i kable podmorskie wymagają takiej samej kontroli i rygorystycznie wdrażanych zabezpieczeń, jak dostęp radiowy i stacje bazowe Być może prace nad opracowaniem zestawów narzędzi dla tych obszarów będą mogły być wykonywane wspólnie.
- Wprawdzie na szczytach NATO w 2021/22 r. stosowano język oparty na niuansach, członkowie sojuszu zgodzili się, że postawa Chin narusza nasze demokratyczne zasady i bezpieczeństwo krajowe. Z uwagi na to wyzwanie systemowe ze strony Chin stało się kluczowym punktem programu NATO, który zyskał na znaczeniu w kontekście zwiększania współpracy w zakresie stosunków rosyjsko-chińskich. Polityka sojuszu w odniesieniu do Chin została zapisana w koncepcji strategicznej, przyjętej na szczycie w Madrycie. Wyzwaniem dla NATO będzie rozwiązanie obecnych zróżnicowanych i wielorakich zagrożeń dotyczących bezpieczeństwa w sposób jednoczesny. Obejmuje to obronę przed atakami hybrydowymi, przełomowe i nowo powstające technologie a także słabą infrastrukturę krytyczną. Ze względu na intensywne zmiany w środowisku związanym z bezpieczeństwem oraz wysokie tempo rozwoju technologicznego, umiejętność osiągnięcia doskonałych wyników w każdym z tych obszarów będzie miała znaczenie kluczowe dla przyszłych sukcesów sojuszu.