GEOPOLITYKA NOWYCH TECHNOLOGII CYFROWYCH

MICHAŁ REKOWSKI, TOMASZ PIEKARZ, BARBARA SZTOKFISZ, ROBERT SIUDAK, IZABELA ALBRYCHT, PRZEMYSŁAW ROGUSKI, PAWEŁ KOSTKIEWICZ, MACIEJ SICIAREK, KRZYSZTOF SILICKI, MAGDALENA WRZOSEK, TOMASZ DYLIK, TEODOR BUCHNER, JOANNA ŚWIĄTKOWSKA, ANDREA G. RODRÍGUEZ, KAMIL MIKULSKI

REDAKCJA: IZABELA ALBRYCHT, MICHAŁ REKOWSKI, KAMIL MIKULSKI

INSTYTUT KOŚCIUSZKI

GEOPOLITYKA
NOWYCH TECHNOLOGII CYFROWYCH

MICHAŁ REKOWSKI, TOMASZ PIEKARZ, BARBARA SZTOKFISZ, ROBERT SIUDAK,
IZABELA ALBRYCHT, PRZEMYSŁAW ROGUSKI, PAWEŁ KOSTKIEWICZ, MACIEJ SICIAREK,
KRZYSZTOF SILICKI, MAGDALENA WRZOSEK, TOMASZ DYLIK, TEODOR BUCHNER,
JOANNA ŚWIĄTKOWSKA, ANDREA G. RODRÍGUEZ, KAMIL MIKULSKI

REDAKCJA: IZABELA ALBRYCHT, MICHAŁ REKOWSKI, KAMIL MIKULSKI

INSTYTUT KOŚCIUSZKI

AUTORZY:

Michał Rekowski
Rywalizacja międzynarodowa w epoce cyfrowej
Tomasz Piekarz
Technologie cyfrowe jako element potęgi mocarstw
Barbara Sztokfisz
Cyberdyplomacja – narzędzie budowania cyfrowego pokoju
Robert Siudak
Nowe podmioty w multilateralnym cyberświecie
Izabela Albrycht
Siła cyfrowych danych
Dr Przemysław Roguski
Geopolityka chmury
Paweł Kostkiewicz, Maciej Siciarek, Krzysztof Silicki, Dr Magdalena Wrzosek
Certyfikacja i standaryzacja w kontekście cyfrowej suwerenności
Tomasz Dylik
Geopolityka cyfrowych pasów i szlaków
Dr hab. Teodor Buchner
Przestrzeń kosmiczna i cyfrowy wyścig zbrojeń
Dr Joanna Świątkowska
Ofensywne działania w cyberprzestrzeni – czynnik kształtujący geopolitykę
Sztuczna inteligencja – paliwo geopolitycznych zmian
Andrea G. Rodríguez
Na szlaku do kwantów: bezpieczeństwo i następstwa gospodarcze informatyki kwantowej
Kamil Mikulski
Znaczenie informacji w rywalizacji geopolitycznej

REDAKCJA: Izabela Albrycht, Michał Rekowski, Kamil Mikulski **KOORDYNACJA**: Michał Rekowski, Kamil Mikulski
KOREKTA: Adam Ladziński, Sebastian Gdela **PROJEKT GRAFICZNY I SKŁAD**: Agnieszka Gogola

PARTNERZY:

Google Microsoft EXATEL NASK

Instytut Kościuszki
ul. Feldmana 4/9-10
31-130 Kraków, Polska
+48 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

SPIS TREŚCI

WPROWADZENIE

Wydarzenia ostatnich kilkunastu miesięcy świadczą jednoznacznie – **nowe technologie cyfrowe (ang. *emerging and disruptive technologies*) stały się jednym z najbardziej zaciętych obszarów rywalizacji mocarstw.**

Toczy się ona głównie wokół dwóch centrów grawitacji – Stanów Zjednoczonych i Chińskiej Republiki Ludowej – w całej rozciągłości łańcuchów wartości, i doprowadzić może nawet do konsekwencji zmieniających oblicze (nie tylko cyfrowego) świata w postaci z jednej strony rozerwania technologicznych łańcuchów dostaw (ang. *decoupling of technological supply chains*), a z drugiej podziału Internetu (ang. Splinternet). W ostatnich tygodniach mogliśmy obserwować szczególne zaostrzenie tej rywalizacji w dwóch ścierających się ze sobą inicjatywach, które mają także potencjał do postrzegania ich jako projekcji „cyfrowej siły" z obu wspomnianych mocarstw. W sierpniu 2020 r. Sekretarz Stanu USA Mike Pompeo ogłosił rozszerzenie programu Czystej Sieci (ang. Clean Network), by zablokować chińskim firmom technologicznym związanym z Chińską Partią Komunistyczną dostęp do rynku i sieci w Stanach Zjednoczonych. Niedługo po tym, we wrześniu odpowiednik Pompeo w Chinach, Wang Yi, ogłosił Globalną Inicjatywę Bezpieczeństwa Danych (ang. Global Initiative on Data Security), by promować chińską wizję zarządzania technologią. I tak oto, konflikt technologiczny między Stanami Zjednoczonymi a Chinami, który wpisuje się w szerszą rywalizację geopolityczną obu krajów, zaczął odgrywać w niej centralną rolę.

Wydarzenia te są jednak wynikiem procesów, które ukształtowały pierwsze dwie dekady XXI wieku. Ofensywne wykorzystanie cyberbroni przeciwko innym państwom pokazały, począwszy od 2007 roku, wydarzenia w Estonii, Gruzji, Iranie i Ukrainie. Skala rewolucji w zdolnościach wywiadowczych, którą umożliwiły nowe narzędzia cyfrowe, wstrząsnęła światową opinią publiczną

w wyniku afery Edwarda Snowdena w 2013 r. Nowe formy manipulacji przy użyciu technologii cyfrowych zostały wykorzystane do naruszenia integralności procesów demokratycznych w najstarszych demokracjach świata, co obserwować mogliśmy podczas wyborów prezydenckich w Stanach Zjednoczonych w 2016 r. Rozpoczęta w 2018 r. globalna debata o dopuszczeniu chińskich firm do rozwoju sieci 5G pokazała doniosłość znaczenia danych cyfrowych i integralności cyfrowej infrastruktury, a także związanych z tym zagrożeń i zależności w technologicznym łańcuchu dostaw. Z kolei rok 2020 przyniósł nam wykładniczy skok wykorzystania cyfrowych technologii we wszystkich aspektach społeczno-gospodarczego funkcjonowania państw, instytucji i biznesu, dobitnie uwidaczniając skalę, doniosłość i różnorodność podatności i słabości cyfrowego świata, w którym żyjemy i żyć będziemy.

Dlatego dziś przywódcy w Ameryce, Europie, Afryce, Azji i Australii otwarcie mówią o suwerenności cyfrowej i autonomii technologicznej, a analitycy i obserwatorzy międzynarodowi ostrzegają, że wspomniany trwały podział cyfrowego świata na antagonistyczne bloki pod przewodnictwem dwóch potęg, Stanów Zjednoczonych i Chin, jest coraz bardziej realny. Globalne procesy zarządzania technologią są dziś obszarem zmagań geopolitycznych, które zmieniają świat. By móc odnaleźć się w tym coraz szybciej ewoluującym krajobrazie zmian i zagrożeń, demokratyczne społeczeństwa w Europie i na świecie potrzebują przede wszystkim dogłębnego zrozumienia natury wyzwań związanych z konsekwencjami rozwoju technologii dla polityki i bezpieczeństwa międzynarodowego. Z tego powodu Instytut Kościuszki i zespół CYBERSEC wraz z grupą znakomitych ekspertów przygotował raport, który dokonuje przeglądu i analizy geopolitycznej roli najważniejszych technologii cyfrowych. Wierząc, że mądre decyzje i skuteczne działania musi poprzedzić zbudowanie prawdziwego i możliwie precyzyjnego obrazu rzeczywistości społecznej oraz świadomości dokonujących się zmian, składamy na Państwa ręce jeden z pierwszych raportów eksperckich poświęconych temu zagadnieniu. Mamy szczerą nadzieję, że będzie on zaczynem do wielu dyskusji, które pomogą skutecznie nawigować decydentom w tym coraz bardziej skomplikowanym świecie, w którym geopolityka nowych technologii odgrywa coraz donioślejszą rolę.

Raport rozpoczynamy rozdziałem Michała Rekowskiego, który omawia **główne elementy rywalizacji amerykańsko-chińskiej w nowej epoce cyfrowej** i rozważa, czy doprowadzi ona do trwałego podziału globalnego Internetu. W kolejnym rozdziale Tomasz Piekarz przedstawia **konceptualizację technologii cyfrowych jako składowej potęgi państw.** W rozdziale trzecim Barbara Sztokfisz omawia zjawisko **cyberdyplomacji** i analizuje najważniejsze działania dyplomatyczne, których przedmiotem jest zarządzanie technologią. Wątek ten kontynuuje w rozdziale czwartym Robert Siudak, przyglądając się **nowym podmiotom pozapaństwowym**, które nie tylko odgrywają kluczową rolę w globalnym krajobrazie technologicznym, ale także coraz aktywniej podejmują działania paradyplomatyczne na forach multilateralnych. W rozdziale piątym Izabela Albrycht przeprowadza brawurową i dogłębną **analizę roli danych cyfrowych jako powietrza, którym oddycha nowy cyfrowy świat, i najcenniejszego zasobu, o który toczy się rywalizacja mocarstw.** Dr Przemysław Roguski w rozdziale szóstym **omawia geopolityczny wymiar chmury obliczeniowej.** Coraz bardziej kluczowe dla cyberbezpieczeństwa państw i gospodarek stają się **procesy standaryzacji i certyfikacj**i, o czym wyczerpująco piszą Krzysztof Silicki, dr Magdalena Wrzosek, Paweł Kostkiewicz i Maciej Siciarek w rozdziale siódmym. Ruch sieciowy nie byłby możliwy bez fizycznej **infrastruktury cyfrowych pasów i szlaków**, których geopolityczne znaczenie dobitnie pokazuje Tomasz Dylik. Cyfryzacja i cyberbezpieczeństwo mają także kluczowe znaczenie dla nowej **rywalizacji geopolitycznej państw w przestrzeni kosmicznej**, co ukazuje dziewiąty rozdział autorstwa dra hab. Teodora Buchnera. Dr Joanna Świątkowska w rozdziale dziesiątym dokonuje aktualnego przeglądu **ofensywnych działań w cyberprzestrzeni** i analizuje, jak kształtują one krajobraz bezpieczeństwa międzynarodowego, a w rozdziale jedenastym omawia geopolityczny wymiar jednej z najważniejszych nowych technologii, jaką jest **sztuczna inteligencja**. W rozdziale dwunastym Andrea Rodríguez rozważa, jak kolejna rewolucyjna technologia – **informatyka kwantowa – zrewolucjonizuje bezpieczeństwo państw**. Raport zamyka rozdział trzynasty, w którym Kamil Mikulski analizuje **funkcje informacji i jej ofensywne wykorzystanie w rozgrywce geopolitycznej mocarstw**.

Zapraszamy Państwa do lektury!

SŁOWO WSTĘPNE

WPŁYW NOWOCZESNYCH TECHNOLOGII NA ŚRODOWISKO MIĘDZYNARODOWE

Dokonująca się obecnie transformacja cyfrowa może być porównywalna jedynie z rewolucją przemysłową, która miała miejsce w dziewiętnastym wieku. Tak jak wtedy silnik parowy oraz mechanizacja produkcji doprowadziły do boomu gospodarczego i przekształceń w społeczeństwach, tak teraz rewolucja cyfrowa zmienia oblicze gospodarek narodowych, funkcjonowanie administracji, wpływa na zachowania społeczne oraz kształtuje relacje międzynarodowe.

Tworząc swego rodzaju „nowy ład", rewolucja cyfrowa niesie ze sobą także zagrożenia. Stąd niejako naturalnie, wraz z opracowywanymi i wdrażanymi kolejnymi innowacyjnymi rozwiązaniami cyfrowymi, pojawiła się kwestia zapewnienia, aby oferowane technologie były bezpieczne. Bez wątpienia przed nami – mam tutaj na myśli nie tylko rządy czy szeroko rozumianą administrację publiczną, lecz także sektor prywatny oraz organizacje pozarządowe – ogromne wyzwanie. I właśnie skala tego wyzwania powoduje, że koniecznością staje się współpraca. Od tego, czy będziemy zdolni wykorzystać potencjały państw, firm, organizacji pozarządowych, zależy, czy cyfrowa rewolucja będzie przebiegać w sposób bezpieczny i niezakłócony. Co ważne, to bezpieczeństwo musi być zapewnione zarówno z perspektywy obywatela, jak i firmy, sektora gospodarki, ale też państwa.

Albowiem z całą pewnością nowoczesne technologie i innowacje zmieniają środowisko międzynarodowe.

Powiedzą Państwo, że to nic nowego, historia dostarcza wielu przykładów, kiedy to innowacje i technologie wpływały na bieg wypadków. W minionym stuleciu technologia nuklearna czy program gwiezdnych wojen miały bezpośredni wpływ na sytuację międzynarodową, zmieniając gwałtownie układ sił. Jednak nawet te spektakularne, przykładowe rozwiązania okazały się być tylko narzędziem wykorzystywanym przez politykę. Tymczasem dzisiaj w coraz większym stopniu procesy polityczne uzależnione są od technologii.

Uzależnienie gospodarek od dostępu do nowoczesnych technologii jest nie tylko źródłem potencjalnej siły politycznej, ale także może stać się źródłem zagrożeń. Szczególnie gdy coraz bardziej zasadne staje się pytanie o rolę i udział gigantów technologicznych w układzie geopolitycznym. Pytanie to musimy zadać zarówno sobie, jak i tym, których ono dotyczy.

Jeszcze kilkadziesiąt lat temu jednym z głównych atrybutów państwa była kontrola arsenału militarnego. To państwa dysponowały najnowocześniejszą i najgroźniejszą bronią. Czy dzisiaj, w dobie rosnącego udziału chociażby rozwiązań bazujących na sztucznej inteligencji nadal możemy powiedzieć, że najgroźniejsza, najbardziej efektywna broń jest w rękach państwa?

Budżety wielkich firm technologicznych są nierzadko na poziomie budżetów państw. Firmy, które

dostarczają usługi globalnie, mają globalne interesy. Tego rodzaju zmiana nie powinna dziwić, ale musimy sobie odpowiedzieć na pytanie o cel. Musimy zdefiniować podstawowe, nadrzędne cele, jakie chcemy osiągnąć, wykorzystując technologię.

Bezsprzecznym jest, że rewolucja cyfrowa przyniosła światu ogromne korzyści, ale najistotniejsze jest to, co jeszcze przed nami. Cyfryzacja nie tylko rozprzestrzenia się na kolejne obszary działalności publicznej oraz na sferę prywatną, lecz wręcz przyspiesza. Transformacja cyfrowa wspiera efektywne modele biznesowe i inwestycje zagraniczne. Dzięki wykorzystywaniu narzędzi powstałych w wyniku postępu technologicznego możemy także skutecznie zadbać o grupy nieuprzywilejowane oraz wykluczone. Aktywność rządu RP w obszarze cyfryzacji pokazuje, że narzędzia cyfrowe pomagają uruchomić potencjał, którego wcześniej brakowało. Mówię zarówno o takich projektach jak Ogólnopolska Sieć Edukacyjna, jak i wspieraniu osób niepełnosprawnych w dostępie do nowych technologii. Odnosi się to do grup społecznych, całych gospodarek, ale i grup państw.

Do tej pory u podstaw tych wszystkich zdobyczy i zmian stały podstawowe wartości świata zachodniego, takie jak: poszanowanie wolności osobistej, poszanowanie zasad demokracji, prawo do swobody wypowiedzi czy demokratyczne i transparentne procesy wyborcze. Nasza cywilizacja koncentruje się na człowieku (human centric). Człowiek jest w centrum zainteresowania nauki, polityki czy kultury. Dlatego dbając o rozwój technologiczny, nie możemy zapominać w wartościach, na których zbudowano podstawy zachodniej cywilizacji. Naszej cywilizacji.

Jeżeli wybierzemy inną drogę i zrezygnujemy z naszych wartości, ryzykujemy, że z pomocą technologii można osiągnąć to, czego nie udało się w przeszłości ustrojom totalitarnym (pełna inwigilacja i kontrola społeczeństwa). Nie możemy podążać drogą obraną przez te państwa, które wykorzystując nowoczesne technologie, jednocześnie ograniczają swobody swoich obywateli.

Musimy wypracować system, w którym wybór wartości to wybór najoptymalniejszy także pod względem gospodarczym. Powinniśmy sobie życzyć, by wybory, które przed nami stoją, były jak najprostsze, żebyśmy nie musieli się zastanawiać, czy godząc się na nowe rozwiązania, nie rezygnujemy z czegoś, co jest dla nas ważne. A dla ludzi Zachodu tymi wartościami są m.in. prawa człowieka i demokracja.

Wierzę, że powinniśmy dążyć do partnerstwa transatlantyckiego opartego na solidarności i zaangażowaniu. Partnerstwa państw, które uważają, że wszyscy mamy prawo do korzystania z otwartego Internetu, do rzetelnych informacji, do niezakłóconej i szanującej prywatność komunikacji drogą elektroniczną.

Możemy i powinniśmy wypracować wspólne rozwiązania i zbudować taki ekosystem cyberbezpieczeństwa, w którym w równym stopniu mamy zaufanie do siebie nawzajem, jak i do technologii, usług i informacji.

Jednym z wyzwań, które staje przed nami jest zdefiniowanie wspólnego modelu bezpieczeństwa sieci 5G. Ale to tylko jeden z obszarów. Tylko jedno z wyzwań.

Marek Zagórski

Sekretarz stanu
w Kancelarii Prezesa Rady Ministrów,
Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Michał Rekowski

RYWALIZACJA MIĘDZYNARODOWA W EPOCE CYFROWEJ

Technologie cyfrowe stanowią nowy obszar rywalizacji państw i warunkować będą wynik trwającej rozgrywki o globalną supremację. Wyścig technologiczny dotyczy zarówno produktów i usług, które pochodzą z rywalizujących ze sobą państw, walczących o dostęp do światowych rynków, jak i konkurencyjnych wizji tego, jak technologia może i powinna być wykorzystywana we wszystkich dziedzinach życia społeczno-gospodarczego – łącznie z polityką. Zarówno te technologie, jak i idee ich wykorzystania stały się także towarem eksportowym. Pozycjonowanie się poszczególnych państw w napędzanej przez technologie rewolucji cyfrowej decydować będzie w nadchodzących latach o ich roli w całym systemie międzynarodowym. Postępująca cyfryzacja przekształca gospodarkę globalną, tworzy zupełnie nowe sektory działalności gospodarczej, modele biznesowe i czynniki wzrostu. Budując nowe połączenia między konsumentami i rynkami, daje państwom i całym regionom szanse na zajęcie wyższej pozycji w globalnych łańcuchach wartości, co pociąga za sobą szybszą modernizację społeczną, wyższe tempo rozwoju gospodarczego i szybszy przyrost dobrobytu[1]. Z tego powodu rywalizacja w obszarze nowych technologii może nie tylko zmienić potencjał gospodarczy czy militarny państwa, ale także przyczynić się do zmiany jego pozycji międzynarodowej i zdolności oddziaływania na innych aktorów systemu.

ZNACZENIE INFRASTRUKTURY I TECHNOLOGII CYFROWYCH DLA GEOPOLITYKI

Infrastruktura cyfrowa stanowi podstawę – kręgosłup i krwiobieg – funkcjonowania cyfrowego

świata. Cyberprzestrzeń w warstwie fizycznej składa się z połączonych kabli, przekaźników radiowych, komputerów, urządzeń sieciowych i wielu innych. Wszystkie one ulokowane są w przestrzeni fizycznej i jako takie podlegają ograniczeniom wynikającym z geografii zarówno fizycznej, jak i politycznej. Dodatkowo, urządzenia te wytwarzane są przez różnych producentów i użytkowane przez rozmaite podmioty, które funkcjonują w odmiennych reżimach politycznych i prawnych. To sprawia, że kontrola nad infrastrukturą cyfrową ma znaczenie geopolityczne. Stanowi także kwestię bezpieczeństwa narodowego i suwerenności państwowej. Potencjalnie – w wypadku kontroli nad infrastrukturą użytkowaną przez wiele podmiotów – wiąże się też z uzyskaniem przewagi wywiadowczej, pozwala bowiem monitorować i ingerować w przesyłane informacje.

Jeśli infrastruktura fizyczna stanowi kręgosłup sieci, to jej warstwa logiczna jest systemem nerwowym, odpowiedzialnym za przepływ pakietów danych. Na warstwę logiczną składają się logiczne połączenia między węzłami sieci: kod, protokoły internetowe, system nazw domen, oprogramowanie i inne nadbudowywane na sobie kolejne poziomy platform (takich jak zbiory danych, komunikatory itp.)[2]. Ponieważ ta warstwa umożliwia aktywną komunikację pomiędzy urządzeniami, które rozpoznają te same protokoły i języki programowania, określa, jakie działania w cyberprzestrzeni są w ogóle możliwe – włączając manipulację tymi urządzeniami. To dzięki niej możliwe jest także użytkowanie sieci i tworzenie rozmaitych aplikacji. Poszerzanie zdolności prowadzenia operacji w warstwie logicznej przekłada się na skuteczniejszą ochronę własnych urządzeń i informacji, ale także na większą możliwość wpływania na urządzenia i informacje kluczowe dla funkcjonowania innych podmiotów. Z tych względów podmioty takie jak państwa (z ich agencjami bezpieczeństwa i wywiadu, siłami zbrojnymi), firmy, grupy hakerskie czy organizacje terrorystyczne rywalizują w rozwoju zdolności działania i kontroli nad cyberprzestrzenią dla realizacji własnych celów: strategicznych, politycznych, gospodarczych i bezpieczeństwa. Rozwój nowych technologii cyfrowych dostarcza potężnych narzędzi dla tej rywalizacji, jednocześnie podnosząc potencjalne koszty porażki. Sieć piątej generacji (5G) przyspieszy rozwój Internetu Rzeczy (ang. *Internet of Things*, IoT), umożliwiając tym samym większą automatyzację procesów gospodarczych i inteligentną transformację miast, zmieniając szczególnie logistykę, transport, spedycję i przemysł. Jednocześnie, z każdym nowym urządzeniem i sensorem podłączonym do sieci wiąże się jednak wzrost liczby podatności na wrogą manipulację, potencjalnie zdolną wyrządzić szkody w świecie fizycznym. Rozwój informatyki kwantowej skutkuje koniecznością przedefiniowania kryptografii, która będzie musiała zmierzyć się z niewyobrażalną dotąd mocą obliczeniową zdolną łamać najbardziej złożone protokoły bezpieczeństwa i szyfrowania danych. Rezultatem będzie potężna asymetria w zdolności obliczeniowej między potęgami dysponującymi zdolnościami kwantowymi a resztą[3], co doprowadzi do powstania podziału w cyfrowym świecie na te podmioty, które rozwiną informatykę kwantową, i te, które będą polegać na dotychczasowych technologiach[a]. Wreszcie Sztuczna Inteligencja (SI) przyniesie dalszą automatyzację i robotyzację kluczowych procesów społecznych i gospodarczych, zmieniając każdą dziedzinę życia społecznego, w tym bezpieczeństwo międzynarodowe. Począwszy od zastosowań militarnych (np. zdolność broni autonomicznej do samodzielnego identyfikowania i atakowania celów), przez obronę w cyberprzestrzeni (automatyczna identyfikacja i neutralizacja ataków skierowanych przeciwko kluczowym systemom danego kraju), a skończywszy na słabo jeszcze poznanym potencjale wywiadowczym (uzyskiwanie cennych informacji wywiadowczych przez zautomatyzowaną analizę dużych wolumenów danych), stosowanie SI w dziedzinie bezpieczeństwa stało się przedmiotem międzynarodowego wyścigu zbrojeń[b]. Jednocześnie, podobnie jak

a Więcej na temat wpływu informatyki kwantowej na stosunki międzynarodowe w rozdziale dwunastym.

b Więcej na temat implikacji SI dla bezpieczeństwa międzynarodowego w rozdziale jedenastym.

rozwój statystyki w XVIII i XIX wieku przyczynił się do rozwoju władzy administracyjnej i wzmocnienia procesów rządzenia w nowożytnym państwie, rozwój SI w XXI wieku przyniesie podobny efekt, pozwalając państwu śledzić, kontrolować i ingerować w obszary życia obywateli i procesy społeczne, które dotąd pozostawały poza zasięgiem nawet najlepiej zorganizowanych biurokracji[4].

TECHNOLOGIE CYFROWE W DOBIE RYWALIZACJI MOCARSTW

Nowe technologie cyfrowe stają się kluczowym obszarem rywalizacji mocarstw o światową dominację, co w minionej dekadzie szczególnie przejawiało się w rosnącej roli, jaką ofensywne działania w cyberprzestrzeni zaczęły odgrywać w polityce zagranicznej i bezpieczeństwa państw, następnie zaś w uczynieniu cyfrowych technologii centralnym obszarem rywalizacji globalnej między Stanami Zjednoczonymi (USA) i Chińską Republiką Ludową (ChRL). Rządy obu tych państw dążą do uzyskania strategicznych przewag w tej sferze oraz starają się wyzwolić od wzajemnej zależności technologicznej, którą postrzegają jako zagrożenie dla bezpieczeństwa narodowego. Szczególne rodzaje wysokich technologii, takie jak informatyka kwantowa, SI czy 5G, postrzegane są jako środki do zmiany globalnej równowagi siły. Ta rywalizacja uległa szczególnej intensyfikacji w ciągu ostatnich kilku lat w związku z zaostrzeniem się konfliktu politycznego i gospodarczego między dwiema potęgami. Od kilku lat Chiny odważnie budują własną potęgę technologiczną. W 2015 roku Pekin przyjął plan Made in China 2025 (chiń. 中国制造2025), który jest strategią rozwoju kluczowych obszarów high-tech chińskiej gospodarki, takich jak robotyka, ICT, energetyka odnawialna czy przemysł lotniczy, w celu przeskoczenia pułapki średniego dochodu i uczynienia z Chin światowego lidera wytwórstwa złożonych i zaawansowanych produktów technologicznych. Strategia zakłada dogłębną modernizację chińskiego przemysłu poprzez budowę zaawansowanych systemów inteligentnej produkcji, ale także wysokie nakłady kapitałowe i działania polityczne uniezależniające Chiny od zagranicznych dostawców sprzętu i technologii. Przewiduje także przejęcia zagranicznych spółek będących liderami innowacji technologicznych, zmierzające do zawłaszczenia najbardziej dochodowych elementów globalnego łańcucha dostaw[5]. Ma zatem na celu **sprawienie, by Chiny stały się samowystarczalne technologicznie, by stały się największym światowym dostarczycielem nowych technologii, oraz by stały się najważniejszym źródłem innowacji.** Chiny chcą więc wkrótce projektować, produkować i eksportować niemal wszystkie najbardziej innowacyjne towary od układów scalonych (jeden z obszarów, gdzie ChRL obecnie jest mocno uzależniona od zagranicznej produkcji[6]) przez samochody elektryczne po roboty i algorytmy gotowe do realizacji zadań w rozmaitych sektorach gospodarki od transportu po edukację. Szczególnie w obszarze robotyki i SI Pekin realizuje swoje globalne ambicje z rozmachem[7]. W 2017 r. Rada Państwa opublikowała nową strategię rozwoju SI (chiń. 新一代人工智能发展规划)[8], która zakłada, że do 2030 r. Chiny staną się największą światową potęgą w zakresie rozwoju i wdrożeń SI[9]. Jak wskazuje Kai-Fu Lee, to Chiny będą największym beneficjentem trwającej obecnie rewolucji technologicznej (i będącej jej konsekwencją rewolucji gospodarczej) związanej z rozwojem SI opartej na „uczeniu głębokim" (ang. *deep learning*). Kai-Fu Lee stwierdza, że w obecnym momencie tego procesu kluczowe jest posiadanie „obfitości danych, głodnych przedsiębiorców, specjalistów od SI i środowiska politycznego przychylnego tej technologii"[10], Chiny zaś spełniają wszystkie te wymogi i pod wieloma względami – np. posiadania skoncentrowanego, dynamicznego i elastycznego środowiska producentów sprzętu elektronicznego jak to skupione w mieście Shenzhen – są niekwestionowanym liderem w skali światowej. Dodatkowo, już dziś Chiny posiadają firmy, których doświadczenie jest kluczowe dla dalszego etapu transformacji cyfrowej napędzanej SI, czy to w zastosowaniu SI przez biznesy internetowe (Alibaba, Tencent) czy w kwestii rozwiązań, które zrewolucjonizują sektory przemysłu i usług publicznych (Baidu, Face++, iFLYTEK). Chińskie firmy stosują także odmienną od technologicznych liderów z Doliny Krzemowej

strategię rywalizacji na obcych rynkach w Europie, Azji, Afryce i Ameryce Południowej. Podczas gdy korporacje amerykańskie stawiają na długoletnie procesy doskonalenia pojedynczych produktów, które jako uniwersalne oferowane są następnie użytkownikom na całym świecie, chińscy giganci technologiczni inwestują w zagraniczne startupy, które bardziej skupiają się na szybkim zajęciu rynku poprzez stworzenie zlokalizowanego produktu, dostosowanego do oczekiwań i wzorców zachowań konsumentów w danym kraju[11]. Pekin aktywnie wspiera także zagraniczną ekspansję swoich firm, m.in. w ramach technologicznego komponentu inicjatywy Pasa i Drogi (chiń. 一带一路), tzw. Cyfrowego Jedwabnego Szlaku (chiń. 数字丝绸之路). Również w zakresie informatyki kwantowej Chiny dokonują znaczących postępów, pracując nad szyframi, których nie będzie dało się złamać[12]. W 2017 r. Chińczycy wykorzystali swojego satelitę do nawiązania między dwoma centrami naziemnymi komunikacji zaszyfrowanej przy użyciu splątania kwantowego[13].

Jedna z głównych osi podziału cyfrowego świata dotyczy prawnych i politycznych aspektów wykorzystania danych. Dane stanowią kluczowy surowiec epoki cyfrowej z dwóch powodówc. Po pierwsze, są ogromnym źródłem informacji o ludzkich działaniach, zachowaniach i preferencjach, a ich agregacja, możliwość skalowania i analizy wielkich zbiorów danych (*Big Data*) otwiera drzwi do potencjalnego rozwiązania ogromnej liczby problemów, z jakimi borykają się społeczeństwa: od wypadków na drogach przez gospodarowanie odpadami po przeciwdziałanie negatywnym konsekwencjom zmian klimatu. Pełen zakres działań, jakie umożliwi analiza *Big Data*, nie jest jeszcze w całości zrozumiany. Po drugie, duże zbiory danych są konieczne do uczenia maszynowego (treningu systemów) i w konsekwencji budowy potężniejszych i bardziej niezawodnych systemów SI. Powszechnie uważa się, że podejście do danych indywidualnych użytkowników w Chinach jest znacznie mniej restrykcyjne niż w Stanach Zjednoczonych czy Unii Europejskiej[14]. Chińskie prawo[15] wymusza na prywatnych firmach współpracę[16] z chińskimi organami bezpieczeństwa narodowego[17]. W Chinach zachodzi więc głęboka synergia pomiędzy wielkimi firmami technologicznymi, które dzięki dominacji lokalnego sprzętu i oprogramowania wśród tamtejszych użytkowników Internetu są w stanie gromadzić ogromne ilości danych, a chińskim rządem, który korzysta z tych danych, włączając z kolei chińskie firmy w ambitne projekty rozwoju inteligentnych usług publicznych, co tworzy im wygodne środowisko do gromadzenia jeszcze większej ilości danych. Jednym z rezultatów takiego stanu rzeczy jest znacznie szybsze tempo rewolucji cyfrowej w Chinach niż w Stanach Zjednoczonych czy Europie[18]. Szczególnie widać to w śmiałości, z jaką technologie cyfrowe znajdują zastosowanie w świecie realnym, fundamentalnie go przekształcając i usprawniając – np. płatności mobilne w Chinach umożliwiły spektakularny rozwój całych gałęzi biznesu korzystających z usług *online2offline*, znacząco ułatwiając życie w chińskich miastach i generując olbrzymie zyski pod dalszy rozwój technologiczny firm i startupów. Podsumowując, **Chiny postrzegają nowe technologie jako narzędzie państwa, które odgrywa kluczową rolę w kształtowaniu jego potęgi. Pod przywództwem Xi Jinpinga centralnego znaczenia nabrało dążenie władz w Pekinie do uczynienia z ChRL technologicznej potęgi, opartej na krajowej produkcji, rozwoju własnych innowacji (chiń. 自主创新) oraz autonomii w zakresie kluczowych technologii[19] (chiń. 核心技术)[20].**

Amerykanie bynajmniej nie podejmują globalnej rywalizacji technologicznej z Chinami z pozycji przegranego. USA są wciąż globalnym liderem w wielu obszarach cyfrowych, a amerykańskie firmy – szczególnie te, które stały się synonimami innowacyjności – mają dziś silną i stabilną pozycję na rynkach świata. W kontekście SI, pomimo prognoz Kai-Fu Lee, należy mieć na uwadze, że niezbędne dla rozwoju aplikacji SI są mikroprocesory obsługujące algorytmy uczenia maszynowego – a jest to obszar, w którym jak dotąd dominują

c Więcej na temat fundamentalnego znaczenia danych w rozdziale piątym.

firmy z USA i państw sojuszniczych[21]. Amerykanie posiadają ok. 45% globalnego rynku półprzewodników i ok. 55[22] przedsiębiorstw zajmujących się produkcją procesorów SI, m.in. Intel, Google, AMD, Qualcomm, Broadcom czy Micron. Inni globalni liderzy w tym zakresie to m. in. tajwański TSMC, koreańskie Samsung i SK Hynix czy japońska Toshiba[23]. Choć Chiny od lat budują krajowy przemysł produkcji półprzewodników (posiadają ok. 25 firm zajmujących się produkcją mikroprocesorów SI), od wymienionych zagranicznych dostawców wciąż pochodzi blisko 84% procesorów używanych w tym kraju – także tych, które trafiają do sprzętu elektronicznego produkowanego przez chińskich gigantów[24]. Przewiduje się, że sprzedaż mikroprocesorów SI będzie rosnąć w kolejnych latach w tempie 35% rocznie i osiągnie 83 miliardy USD w roku 2027[25]. W lutym 2019 r. prezydent Trump wydał rozporządzenie wykonawcze, które wzywa rząd federalny do odegrania proaktywnej roli w utrzymaniu statusu lidera SI przez Stany Zjednoczone[26]. Dokument nadaje SI priorytet wśród planów amerykańskich instytucji badawczo-rozwojowych, przewiduje także szeroki zakres działań – od pogłębienia synergii między rządowymi i pozarządowymi centrami rozwoju SI przez wdrożenie regulacji ułatwiających rozwój SI po zwiększanie odpowiednich kompetencji wśród amerykańskich pracowników. Podobne kroki podjęto również w zakresie innych technologii – m.in. w 2018 r. przyjęto ustawę o narodowej inicjatywie kwantowej (ang. National Quantum Initiative Act), którego celem jest wsparcie działań mających zapewnić USA pozycję lidera informatyki kwantowej[27].

Waszyngton postrzega technologiczne ambicje Pekinu jako zagrożenie dla swojej mocarstwowej pozycji i bezpieczeństwa narodowego[28]. Obecna administracja Donalda Trumpa stawia czoła wyzwaniu ze strony rosnącej chińskiej potęgi technologicznej. Jeszcze w 2018 r. Trump podpisał nowelizację budżetu obronnego (National Defense Authorization Act, NDAA), która zakazała administracji USA korzystania ze sprzętu produkowanego przez szereg chińskich firm z Huawei i ZTE na czele. Wkrótce Huawei stał się głównym celem amerykańskich działań, gdy w grudniu 2018 r. główna księgowa tej firmy i córka założyciela, Meng Wanzhou, została aresztowana na lotnisku w Vancouver na wniosek organów ścigania USA. Następnie w maju 2019 r. Departament Handlu umieścił Huawei na liście podmiotów obłożonych restrykcjami, co poskutkowało m.in. zawieszeniem współpracy Google'a z tą firmą, obejmującej transfer technologii, sprzętu i usług związanych z systemem operacyjnym Android, z którego korzystały produkty Huawei[29]. Huawei stanowi szczególne wyzwanie dla Waszyngtonu, gdyż jest jednym z czołowych globalnych dostawców sprzętu do budowy sieci 5G, na której opierać się będzie infrastruktura krytyczna przyszłości. **Amerykanie postrzegają budowę infrastruktury pod 5G z wykorzystaniem chińskiego sprzętu jako żywotne zagrożenie dla bezpieczeństwa narodowego[30].** Stąd od 2018 r. prowadzą szeroko zakrojone działania dyplomatyczne na rzecz przekonania swoich sojuszników na całym świecie o konieczności wykluczenia chińskich dostawców sprzętu 5G z krajowych planów budowy sieci[d]. Wyżej wspomniane regulacje miały też osłabić międzynarodową pozycję Huawei w wymiarze ekspansji technologii. W kwietniu 2020 r. Sekretarz Stanu Mike Pompeo ogłosił, że cały ruch sieciowy 5G z i do USA będzie musiał stosować zasadę „czystej ścieżki" (ang. *Clean Path*), przewidzianej w NDAA z 2019 r., która wzmocniła zakaz korzystania z chińskiego sprzętu i usług nałożony na instytucje rządowe w USA[31]. Z kolei w połowie 2020 r. administracja Trumpa skupiła się na TikToku, popularnej wśród młodzieży aplikacji społecznościowej stworzonej przez chińską firmę ByteDance, co do której kilka miesięcy wcześniej[32] pojawiły się obawy, że zagraża prywatności danych

d Więcej na ten temat: Albrycht I., Świątkowska J., *5G Made by America*, brief programowy, Instytut Kościuszki, 08.2020, [online:] https://ik.org.pl/wp-content/uploads/ik_brief_programowy_5g_madebyamerica_v4.pdf; Albrycht I., Świątkowska J., *THE FUTURE OF 5G OR QUO VADIS, EUROPE?*, brief programowy, Instytut Kościuszki, 07.2019 [online:] https://ik.org.pl/wp-content/uploads/ik_policy_brief_5g_eng.pdf.

użytkowników, które mogą być udostępniane chińskim władzom[33]. W odpowiedzi na te wątpliwości Trump wydał rozporządzenie wykonawcze[34], które po upływie 45 dni zakazuje amerykańskim obywatelom i firmom dokonywania jakichkolwiek transakcji z ByteDance, w efekcie eliminując możliwość użytkowania aplikacji przez Amerykanów. Podobne rozporządzenie zostało wydane w odniesieniu do aplikacji WeChat[35], zaś Mike Pompeo zasugerował, że lista chińskich aplikacji budzących podobne obawy władz USA jest znacznie dłuższa[36].

Najważniejszym elementem amerykańskich działań wymierzonych w Chiny jest dążenie do tzw. *decouplingu* – rozerwania i przeniesienia globalnych łańcuchów wartości, które szczególnie w dziedzinie technologii wiążą gospodarkę amerykańską (i szerzej globalną) z Chinami. W pierwszej połowie 2020 r. proces decouplingu znacząco przyspieszył w związku z opanowującą świat pandemią wirusa SARS-CoV-2. Po pierwsze, w wyniku rozprzestrzeniania się koronawirusa rządy niemal wszędzie na świecie podjęły decyzję o zamknięciu granic i zamrożeniu niektórych sektorów gospodarki. Konsekwencją było faktyczne zatrzymanie globalnych przepływów ludzi, towarów i usług w obszarach, gdzie swoboda zachodzenia takich przepływów była dotąd traktowana jako gwarantowany i nieusuwalny element świata społecznego i gospodarczego[37]. W związku z restrykcjami wprowadzonymi w chińskich prowincjach, gdzie skupiona jest globalna produkcja wielu dóbr, fabryka świata stanęła, co skutkowało opóźnieniem planów sprzedaży najnowszego sprzętu czołowych producentów, m.in. nowego iPhone'a[38]. Po drugie, w ten sposób pandemia uwydatniła zależność państw i gospodarek od transnarodowych łańcuchów dostaw w wielu strategicznych obszarach takich jak zasoby medyczne czy sprzęt technologiczny[39]. Ten efekt dodatkowo nałożył się na rosnące od pewnego czasu obawy w USA i Europie przed chińskimi inwestycjami w strategiczne obszary gospodarki na obu kontynentach, szczególnie zaś w nowe technologie[40]. Waszyngton zrozumiał wyjątkowość tego momentu i postanowił wykorzystać chwilowe spowolnienie procesów globalizacyjnych, by zintensyfikować politykę decouplingu – m.in. w maju Keith Krach, podsekretarz w Departamencie Stanu, stwierdził, że USA rozpoczęły „turbodoładowanie tej inicjatywy"[41]. W tym procesie kluczowe jest współdziałanie amerykańskich sojuszników i państw podobnie myślących – stąd amerykańska dyplomacja rozpoczęła narrację o budowie Sieci Dobrobytu Gospodarczego (ang. Economic Prosperity Network). Dążenie do przebudowania łańcuchów dostaw, tak by w miarę możliwości omijały Chiny i chińskie firmy, wymaga udziału firm, rządów, instytucji i organizacji pozarządowych z innych obszarów świata – poza USA i Chinami. Sieć Dobrobytu Gospodarczego odnosi się do nowej idei współpracy ekonomicznej między tymi podmiotami, promowanej od kilku miesięcy przez Departament Stanu i opartej na współdzielonych wartościach: uczciwości, odpowiedzialności, wzajemności, a także poszanowaniu dla rządów prawa, własności, suwerenności i praw człowieka[42]. Relokacja łańcuchów dostaw poza Chiny jest atrakcyjna dla regionów rozwijających się, dla których może oznaczać napływ inwestycji zagranicznych, budowę nowej infrastruktury i liberalizację handlu, co przełoży się na przyspieszony rozwój gospodarczy[43]. Z dużym prawdopodobieństwem wyznacznikiem partnerstw i kierunków współdziałania w tym zakresie będzie dla Waszyngtonu reakcja państw sojuszniczych na wezwania do wykluczenia chińskich producentów sprzętu do budowy sieci 5G. Lista urzędujących przywódców, którzy stopniowo zajmują coraz bardziej stanowcze stanowisko w tej kwestii, rośnie[44]. Pomimo to całkowite rozerwanie łańcuchów dostaw zaczynających się w Chinach będzie bardzo trudne do przeprowadzenia, a negatywne konsekwencje takiego procesu dotkną także amerykańskie firmy i amerykańskich konsumentów[45]. Tym niemniej **Waszyngton coraz intensywniej stara się mobilizować swoich sojuszników, by zbudować nowy sojusz demokracji[46], którego celem ma być wspólne stawienie czoła Chinom we wszystkich obszarach – włączając technologie cyfrowe.** W tym duchu w sierpniu 2020 r. Mike Pompeo ogłosił rozszerzenie programu Czystej Sieci (ang. The Clean Network), który **dąży do rozerwania technologicznych więzi między USA i ChRL nie tylko w kwestii 5G. Przewiduje on, iż chińskie firmy – m.in. operatorzy telefonii komórkowych, producenci aplikacji i oprogramowania czy dostawcy usług w chmurze – utracą dostęp do szeroko rozumianego rynku w Stanach Zjednoczonych[47]. Celem inicjatywy jest także zapewnienie, by infrastruktura cyfrowa świata nie stała się przedmiotem złośliwej bądź szpiegowskiej działalności ze strony ChRL.**

BITWA O PRZYSZŁOŚĆ INTERNETU – W STRONĘ SUWERENNOŚCI CYFROWEJ

Rozwój globalnego Internetu umożliwił swobodny przepływ danych na niewyobrażalną uprzednio skalę, doprowadzając do demokratyzacji wszystkich form wykorzystania i zastosowania informacji. W efekcie państwa utraciły monopol na czerpanie zysków z najważniejszych owoców i największych korzyści rewolucji cyfrowej. Obecnie muszą one konkurować z innymi podmiotami, takimi jak choćby prywatne korporacje[e], które nierzadko są od nich znacznie bardziej zaawansowane w rozwoju nowych technologii, znacznie lepiej pozycjonowane do wdrażania ich nowatorskich zastosowań i znacznie lepiej przygotowane do prowadzenia konfliktu w cyberprzestrzeni (zarówno w sensie ofensywnym, jak i defensywnym). W ciągu ostatnich dwóch dekad trend ten szczególnie dał się we znaki rządom wraz z szybkim rozwojem technologii cyfrowych i coraz szerszymi obszarami ich użycia. Nie ominął także ich kolebki, czyli Stanów Zjednoczonych. Choć Internet powstał jako projekt amerykańskiego rządu na użytek wojska, przez krótki okres po zakończeniu zimnej wojny amerykańskie firmy technologiczne mogły rozwinąć się jako prawdziwie globalne korporacje budujące uniwersalny Internet światowy dający dostęp do informacji i usług cyfrowych każdemu, kto wszedł w posiadanie komputera i łącza sieciowego. Wypadki kolejnych lat – szczególnie zaś ataki z 11 września 2001 r., wojna w Iraku i wyzwania kontrwywiadowcze stojące przed amerykańską wspólnotą bezpieczeństwa – sprawiły, że instytucje federalne na nowo zainteresowały się działalnością amerykańskich gigantów technologicznych[48]. Rewelacje upublicznione w wyniku afery Edwarda Snowdena w 2013 r. zwróciły uwagę opinii publicznej na fakt, że największe amerykańskie korporacje technologiczne *de facto* zostały potraktowane instrumentalnie przez instytucje bezpieczeństwa tego kraju, jako narzędzia w procesie realizacji interesów strategicznych. Odcisnęły także piętno na myśleniu przywódców innych państw o roli, jaką technologie cyfrowe odgrywają w budowaniu potęgi państwowej i suwerennej kontroli nad ich społeczeństwami.

Ten trend powoli zrodził reakcję zwrotną ze strony państw, wśród których najsilniejsze zaczynają dążyć do realizacji koncepcji suwerenności cyfrowej. Ponieważ technologie cyfrowe w sposób fundamentalny podważają suwerenność i dominację instytucji państwowych (lub utworzonych przez nie instytucji międzynarodowych), suwerenność cyfrowa ma wyznaczać wektor działań zmierzających do uzyskania suwerennej kontroli tych instytucji nad cyberprzestrzenią. W ciągu ostatniej dekady koncepcja ta zaczęła zyskiwać popularność w państwach tradycyjnie przywiązanych do silnego akcentowania swojej niepodległości, takich jak Francja czy Chiny, a od niedawna stanowi także element polityki Unii Europejskiej, choć w Europie rozumiana jest inaczej niż w Chinach. Europejskie działania na rzecz suwerenności cyfrowej[f] stawiają w centrum obywateli, i jako takie dążą do zabezpieczenia i wzmocnienia ich praw i pozycji w cyfrowym świecie. W przypadku UE idea suwerenności cyfrowej jest związana z szerszą koncepcją Europejskiej Autonomii Strategicznej, która odnosi się do niezakłóconej przez czynniki zewnętrzne swobody w definiowaniu i realizacji celów Europy jako podmiotu na arenie międzynarodowej. Europejska Autonomia Strategiczna obejmuje działania realizowane w całym spektrum

e Więcej na ten temat w rozdziale czwartym.

f Więcej na temat europejskich działań na rzecz suwerenności cyfrowej w odniesieniu do danych w rozdziale szóstym.

sektorów polityk, od polityki obronnej i bezpieczeństwa, zagranicznej, przemysłowej, technologicznej po kosmiczną czy zdrowotną (konieczność budowania autonomii strategicznej w tym ostatnim obszarze szczególnie uwypuklona została w trakcie pandemii COVID-19). Autonomia strategiczna w obszarze technologicznym oznacza zatem swobodę w kształtowaniu tego obszaru wedle własnych zasad i celów, i jako koncepcja suwerenności technologicznej (ang. *technological sovereignty*) znalazła się w oficjalnym programie nowej przewodniczącej Komisji Europejskiej, Ursuli von der Leyen[49]. Z kolei obecny Komisarz ds. Rynku Wewnętrznego Thierry Breton często[50] posługuje się francuską[g] **koncepcją suwerenności cyfrowej (fr. *souveraineté numérique*), która oznacza zdolność do: swobodnego wyznaczania celów i działania w cyberprzestrzeni, suwerennej kontroli nad narzędziami cyfrowymi, a także zachowania tradycyjnych obszarów suwerenności państwowej w obliczu wyzwań wynikających z cyfryzacji**[51]. W tym ujęciu koncepcja suwerenności cyfrowej jest węższa od **koncepcji suwerenności technologicznej, gdyż ta druga odnosi się także do zagadnień np. polityki handlowej (bezpieczeństwo łańcuchów dostaw), przemysłowej (budowa bazy technologiczno-przemysłowej) czy stosowania technologii w branżach strategicznych (np. polityka kosmiczna).** Koncepcja suwerenności cyfrowej odgrywa także kluczową rolę w polityce technologicznej Chin. Pekin postrzega rozwój Internetu jako jeden z kluczowych procesów globalizacyjnych, które przynoszą zmianę i zamęt społeczny. Ekspansja sieci w oczach chińskich decydentów wymaga zdecydowanych działań, które okiełznają jej negatywne konsekwencje – wymaga zarządzania, którego podmiotami mają być rządy narodowe. Suwerenność jest nadrzędną wartością określającą ramy rozwoju Internetu w Chinach, który znajduje się pod państwową jurysdykcją i podlega państwowemu prawu. Chiny uznają zatem globalny Internet za sumę składowych – narodowych części, podlegających prawodawstwu poszczególnych krajów. Między innymi z tego powodu Pekin wspiera Organizację Narodów Zjednoczonych w jej wysiłkach na rzecz zarządzania Internetem[52]. ONZ zrzesza państwa, Pekin zaś dąży do legitymizacji światowego konsensusu politycznego w sprawie takiego modelu Internetu, w którym najsilniejszymi podmiotami – jego lokalnymi zarządcami i suwerenami – będą rządy narodowe[53]. Taka wizja organizacji sieci faworyzuje państwa kosztem pozycji aktorów pozapaństwowych (np. korporacji czy organizacji pozarządowych) oraz jednostek (obywateli)[54]. By promować swoją wizję Internetu, w 2014 r. Chiny uruchomiły w Wuzhen własne coroczne forum poświęcone globalnemu zarządzaniu Internetem, World Internet Conference (世界互联网大会)[55]. Podczas ceremonii otwarcia wydarzenia w 2015 r. przewodniczący Xi Jinping mówił o suwerenności cyfrowej (网络主权 – wăngluò zhǔquán – co można tłumaczyć także jako suwerenność internetową lub cybersuwerenność). Wedle tej koncepcji państwo uprawnione jest do wyznaczania suwerennych granic w obrębie Internetu, w ramach których sprawuje niepodzielną władzę[56]. Innymi słowy, cybersuwerenność w tej wersji oznacza podporządkowanie Internetu i szerzej technologii cyfrowych interesowi państwa. W praktyce przekłada się to na podporządkowanie przede wszystkim użytkowników i dostawców usług cyfrowych operujących na danym terytorium krajowej władzy ustawodawczej i wykonawczej. Docelowo odbywać ma się to bez względu na fakt, czy dany podmiot – indywidualny użytkownik czy międzynarodowa korporacja – posiada obce obywatelstwo czy siedzibę w innym państwie. W 2010 r. Rada Państwa wydała Białą Księgę zatytułowaną *Internet w Chinach* (chiń. 中国互联网状况), gdzie rozwój i zarządzanie Internetem uznane zostało za kwestię dotyczącą dobrobytu i rozwoju narodowego, a także suwerenności i bezpieczeństwa państwa[57]. Taka logika „cybersuwerenności" już w latach 90. XX wieku wyznaczała kierunek rozwoju dwóch głównych chińskich

g Zarówno koncepcję suwerenności cyfrowej, jak i autonomii strategicznej stworzono i rozwinięto we Francji. Obie współdzielą podobną drogę – chociaż pierwotnie powstały w odniesieniu do suwerenności Republiki Francuskiej, stopniowo zostały przeniesione na grunt europejski, zapładniając intelektualnie kierunki rozwoju polityki bezpieczeństwa czy cyfrowej w Unii Europejskiej.

przedsięwzięć zajmujących się administrowaniem Internetem: Wielkiego Firewalla (chiń. 防火长城), który za pomocą środków prawnych, rozwiązań technologicznych i nacisków politycznych na dostarczycieli usług blokuje w Chinach dostęp do niepożądanych stron, oraz Projektu Złota Tarcza (chiń. 金盾工程), który jest systemem nadzoru nad ruchem sieciowym w Chinach[58]. Koncepcja suwerenności cyfrowej wykracza jednak poza samą kwestię zarządzania siecią i obejmuje szerokie spektrum znaczenia technologii cyfrowych dla rozwoju i bezpieczeństwa narodowego. Oznacza na przykład, że dane pozyskiwane od podmiotów znajdujących się na terytorium danego państwa powinny być przechowywane w repozytoriach również ulokowanych w obrębie jego granic.

Trend ustanawiania pełnej suwerenności cyfrowej najważniejszych aktorów państwowych i regionalnych prowadzić może do powstania *Splinternetu* – podziału globalnego Internetu na sieci lokalne (regionalne i państwowe), nad którymi instytucje polityczne państwa sprawują suwerenną kontrolę[59]. Każdy z tak wytyczonych obszarów Internetu mógłby zostać zorganizowany wedle innych reguł, odpowiadających wizji politycznej danych władz. Rząd zdecyduje o tym, co, kiedy i jak w sieci będzie można zrobić – jakie strony odwiedzać, jakie treści publikować, jakie informacje przesyłać i jakie dane udostępniać. Z konieczności przyniosłoby to fragmentaryzację Internetu[60] – w tak skrajnie dystopijnej wizji w różnych częściach świata obowiązywać będą nie tylko odmienne regulacje dotyczące korzystania z sieci i odmienne prawo związane z bezpieczeństwem przesyłu informacji, ale także odmienne rozwiązania sprzętowe i programowe – de facto odmienne technologie. Oznaczać będzie to koniec uniwersalnego Internetu, który przestanie być ogólnoświatową agorą umożliwiającą interakcję każdego z każdym i swobodną wymianę danych. Zamiast niego użytkownicy z różnych państw skazani będą na korzystanie z lokalnych Intranetów, będących cyfrowymi odpowiednikami tego, co dzieje się w ich granicach terytorialnych. **Postępująca fragmentaryzacja Internetu odbija przekształcenia obecnego systemu międzynarodowego, który staje się coraz bardziej wielobiegunowy, a władza w nim ulega dekoncentracji geograficznej. Ale rywalizacja największych potęg międzynarodowych nie odnosi się wyłącznie do różnych wizji organizacji Internetu, lecz dotyczy całości roli technologii we współczesnym świecie.**

Stany Zjednoczone jako kraj o silnych tradycjach wolności indywidualnej predestynowany jest do przewodzenia demokratycznemu nurtowi zarządzania technologią, który stawia ograniczenia wzmocnionej władzy państwa względem wolności obywatelskich[61]. Choć amerykańska wspólnota wywiadowcza w ostatnich dwóch dekadach zyskała wizerunek wszechszpiegującego molocha, w USA funkcjonuje demokratyczna kontrola zarówno aparatu bezpieczeństwa, jak i firm technologicznych. Wiele społeczeństw świata przywiązanych do demokratycznych wartości i praw człowieka dąży do przyjęcia regulujących technologie rozwiązań, które będą wspierać te pryncypia – USA pozostaną ich naturalnym – i niezbędnym – sojusznikiem. Oczywistym partnerem USA w tym kontekście będzie Unia Europejska, ale także ich demokratyczni sojusznicy z krajów Five Eyes oraz Japonia, Korea Południowa czy Indie. **Demokratyczne państwa, które myślą podobnie o relacji techniki i społeczeństwa, nie powinny naśladować chińskiego modelu rozwoju i wykorzystania technologii. Zamiast tego powinny skupić się, by wspólnie pokierować trwającą rewolucją technologiczną w sposób, który sprawi, że ochroni ona i wzmocni najważniejsze dla nich wartości demokracji i swobód indywidualnych.** Także Unia Europejska, podążając własną ścieżką tożsamości technologicznej w celu budowy Europejskiej Autonomii Strategicznej, może tworzyć globalną synergię z USA oraz wspomnianymi państwami, tym sposobem kładąc zręby pod bardziej demokratyczny i przyjazny obywatelom cyfrowy świat.

PRZYPISY

1 Khanna P., *Connectography. Mapping the Global Network Revolution*, W&N, London 2016, s. 158–163.

2 Clark D., *Characterizing cyberspace: past, present and future*, MIT CSAIL, 12.03.2010, [online:] https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf.

3 Rodriguez A. G., Padilla A. M., Siudak R., *POST-QUANTUM INTERNATIONAL SECURITY. An Introduction*, Policy Brief, The Kosciuszko Institute, 02.2020 [online:] https://ik.org.pl/wp-content/uploads/ik_policy_brief_post-quantum-international-security.pdf.

4 Wright N., *How Artificial Intelligence Will Reshape the Global Order. The Coming Competition Between Digital Authoritarianism and Liberal Democracy*, Foreign Affairs, 10.07.2018.

5 Wubekke J., Meissner M., Zenglein M. J., Ives J., Conrad B., *MADE IN CHINA 2025. The making of a high-tech superpower and consequences for industrial countries*, Mercator Institute for China Studies, MERICS Papers on China, No 2, December 2016, s. 8.

6 Lewis J. A., *China's Pursuit of Semiconductor Independence*, Center for Strategic & International Studies, 27.02.2019, [online:] https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence.

7 Witchalls C., *China is catching up to the US on artificial intelligence research*, The Conversation, 27.02.2019, [online:] https://theconversation.com/china-is-catching-up-to-the-us-on-artificial-intelligence-research-112119.

8 新一代人工智能发展规划的通知, The State Council of the People's Republic of China, 8.07.2017, [online:] http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

9 Webster G., Creemers R., Triolo P., Kania E., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)*, New America, 01.08.2017, [online:] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

10 Lee K. F., *Inteligencja sztuczna, rewolucja prawdziwa*, Media Rodzina, 2019, s. 28.

11 Tamże, s. 168–170.

12 Kania E. B., Costello J., *Quantum Hegemony? China's Ambitions and the challenge to U.S. Innovation Leadership*, Center for a New American Security, 12.09.2018, [online:] https://www.cnas.org/publications/reports/quantum-hegemony.

13 Kwon K., China Reaches *New Milestone in Space-Based Quantum Communications*, Scientific American, 25.06.2020, [online:] https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/.

14 Jaishankar D., *From the iPhone to Huawei: The new geopolitics of technology*, Brookings, 31.07.2019, [online:] https://www.brookings.edu/blog/order-from-chaos/2019/07/31/from-the-iphone-to-huawei-the-new-geopolitics-of-technology/.

15 Wang Z., *Systematic Government Access to Private-Sector Data in China*, [w:] Cate F. H., Dempsey J. X., *Bulk Collection: Systematic Government Access to Private-Sector Data*, Oxford Scholarship Online, 2017, [online:] https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11.

16 Hvistendahl M., *How China surveils the world*, MIT Technology Review, 19.08.2020, [online:] https://www.technologyreview.com/2020/08/19/1006455/gtcom-samantha-hoffman-tiktok/.

17 Wagner J., *China's Cybersecurity Law: What You Need to Know*, The Diplomat, 01.06.2017, [online:] https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ .

18 Macaes B., *The Dawn of Eurasia*, Allen Lane, 2018, s. 116-117.

19 Creemers R., Triolo P., Webster G., *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference*, New America, 30.04.2018, [online:] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

20 Triolo P., Webster G., Tai K., *Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities*, New America, 01.05.2018, [online:] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

21 Buchanan B., *The U.S. Has AI Competition All Wrong*, Foreign Affairs, 07.08.2020, [online:] https://www.foreignaffairs.com/articles/united-states/2020-08-07/us-has-ai-competition-all-wrong.

22 *The Deloitte Research Monthly Outlook and Perspectives, Issue LII*, Deloitte, 01.11.2019, [online:] https://www2.deloitte.com/cn/en/pages/about-deloitte/articles/deloitte-research-issue-52.html.

23 Marco Polo, *AI Chips*, 2020, [online:] https://macropolo.org/digital-projects/supply-chain/ai-chips/ai-chips-supply-chain-mapping/.

24 Daxue Consulting, *China's Semiconductor Industry: 60% of the global semiconductor consumption*, 26.03.2020, [online:] https://daxueconsulting.com/chinas-semiconductor-industry/.

25 Marco Polo, *AI Chips*, 2020, [online:] https://macropolo.org/digital-projects/supply-chain/ai-chips/ai-chips-supply-chain-mapping/.

26 *Executive Order on Maintaining American Leadership in Artificial Intelligence*, The White House, 11.02.2019, [online:] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

27 *National Quantum Initiative Act*, United States Congress, 21.12.2018, [online:] https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf.

28 Murray B., *The Great Decoupling? What's Next for U.S.-China Rift*, Bloomberg, 15.06.2020, https://www.bloomberg.com/news/articles/2020-06-15/the-great-decoupling-what-s-next-for-u-s-china-rift-quicktake .

29 Moon A., *Exclusive: Google suspends some business with Huawei after Trump blacklist – source*, Reuters, 19.05.2019, [online:] https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB.

30 Kania E., *Securing Our 5G Future. The Competitive Challenge and Considerations for U.S. Policy*, Center for a New American Security, 07.11.2019, [online:] https://www.cnas.org/publications/reports/securing-our-5g-future.

31 *Secretary Michel R. Pompeo At a Press Availability*, United States Department of State, 29.04.2020, [online:] https://www.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/.

32 Nicas J., Isaac M., Swanson A., *TikTok Said to Be Under National Security Review*, The New York Times, 01.11.2019, [online:] https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

33 Matsakis L., *Does TikTok Really Pose a Risk to US National Security?*, WIRED, 17.07.2020, [online:] https://www.wired.com/story/tiktok-ban-us-national-security-risk/.

34 *Executive Order on Addressing the Threat Posed by TikTok*, The White House, 06.08.2020, [online:] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

35 Moshin S., Banjo S., *Trump Signs Executive Orders Barring Transactions With TikTok and WeChat in 45 Days*, Time, 6.08.2020, https://time.com/5877214/tiktok-donald-trump-executive-order/.

36 Czuczka T., *U.S. to act on China software beyond TikTok, Pompeo says*, Los Angeles Times, 02.02.2020, [online:] https://www.latimes.com/world-nation/story/2020-08-02/pompeo-says-trump-to-take-broad-action-on-chinese-software.

37 Johnson K., Gramer R., *The Great Decoupling*, Foreign Policy, 14.05.2020, [online:] https://foreignpolicy.com/2020/05/14/china-us-pandemic-economy-tensions-trump-coronavirus-covid-new-cold-war-economics-the-great-decoupling/.

38 Kubota Y., *Apple Delays Mass Production of 2020 Flagship iPhones*, The Wall Street Journal, 27.04.2020, [online:] https://www.wsj.com/articles/apple-delays-mass-production-of-2020-flagship-iphones-11587984138.

39 Hille K., McMorrow R., Liu Q., *Coronavirus shakes centre of world's tech supply chain*, Financial Times, 05.02.2020, [online:] https://www.ft.com/content/22345198-47e6-11ea-aeb3-955839e06441.

40 *Statement by President von der Leyen at the joint press conference with President Michel, following the EU-China Summit videoconference*, European Commission, 22.06.2020, [online:] https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1162.

41 Pamuk H., Shalal A., *Trump administration pushing to rip global supply chains from China: officials*, Reuters, 04.05.2020, [online:] https://www.reuters.com/article/us-health-coronavirus-usa-china/trump-administration-pushing-to-rip-global-supply-chains-from-china-officials-idUSKBN22G0BZ.

42 *Under Secretary Keith Krach Briefs the Press on Huawei and Clean Telcos*, United States Department of State, 25.06.2020, [online:] https://www.state.gov/telephonic-briefing-with-keith-krach-under-secretary-for-economic-growth-energy-and-the-environment/.

43 Ying M., *Traders are rewriting strategies for post-virus Asia Stocks*, Bloomberg, 13.05.2020, [online:] https://www.bloomberg.com/news/articles/2020-05-12/traders-are-rewriting-strategies-for-post-epidemic-asia-stocks.

44 Calhoun G., *Is The UK Ban On Huawei The "Endgame" For Free Trade?*, Forbes, 24.07.2020, [online:] https://www.forbes.com/sites/georgecalhoun/2020/07/24/is-the-uk-ban-on-huawei-the-endgame-for-free-trade/#527cf0b846db.

45 Liang Y., *The US, China and the Perils of Post-COVID Decoupling*, The Diplomat, 08.05.2020, [online:] https://thediplomat.com/2020/05/the-us-china-and-the-perils-of-post-covid-decoupling/ .

46 Yong C., *Pompeo calls on 'free nations' to stand up to China in major speech*, Straits Times, 24.07.2020, [online:] https://www.straitstimes.com/world/united-states/pompeo-calls-for-free-world-to-triumph-over-chinas-new-tyranny.

47 *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, United States Department of State, 05.08.2020, [online:] https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets//.

48 Malcomson S., *Splinternet. How Geopolitics and Commerce Are Fragmenting the World Wide Web*, OR Books, 2016, s. 103.

49 von der Leyen U., *A Union that strives for more. My agenda for Europe*, European Commission, 06.2020, [online:] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

50 Cf. Guillermard V., *Thierry Breton: «Il faut assurer la souveraineté numérique de l'Europe»*, „Le Figaro", 01.07.2020, [online:] https://www.lefigaro.fr/societes/thierry-breton-il-faut-assurer-la-souverainete-numerique-de-l-europe-20200701; *Thierry BRETON auditionné sur la souveraineté numérique*, Sénat, 28.05.2019, [online:] https://www.senat.fr/presse/cp20190528a.html; Vitard A., *Pour Thierry Breton, l'UE doit avoir sa propre constellation de satellites pour l'internet haut debit*, 06.2020, [online:] https://www.usine-digitale.fr/amp/editorial/pour-thierry-breton-l-ue-doit-avoir-sa-propre-constellation-de-satellites-pour-l-internet-haut-debit.N981916.

51 *Le devoir de souveraineté numérique, Sénat*, [online:] http://www.senat.fr/rap/r19-007-1/r19-007-17.html.

52 China Daily, *Full Text: White paper on the Internet in China*, 08.06.2010, [online:] https://www.chinadaily.com.cn/china/2010-06/08/content_9950198_8.htm.

53 Segal A., *When China Rules the Web. Technology in Service of the State*, Foreign Affairs, Vol. 97, No 7, s. 16-17.

54 Tiezzi S., *China's 'Sovereign Internet'*, The Diplomat, 24.06.2014, [online:] https://thediplomat.com/2014/06/chinas-sovereign-internet/.

55 Tiezzi S., *The Internet with Chinese Characteristics*, The Diplomat, 20.11.2014, [online:] https://thediplomat.com/2014/11/the-internet-with-chinese-characteristics/.

56 Tiezzi S., *China Vows No Compromise on 'Cyber Sovereignty'*, The Diplomat, 16.12.2015, [online:] https://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty/.

57 China Daily, *Full Text: White paper on the Internet in China*, 08.06.2010, [online:] https://www.chinadaily.com.cn/china/2010-06/08/content_9950198_8.htm.

58 Hunt P., *China's Internet Policy Offers the Wrong Kind of Lessons*, The Diplomat, 07.06.2016, [online:] https://thediplomat.com/2016/06/chinas-internet-policy-offers-the-wrong-kind-of-lessons/.

59 Pandya J., *Geopolitics of Cybersecurity. Implications for the Future of Humanity*, Risk Group, 2020, s. 94.

60 Gueham F., *DIGITAL SOVEREIGNTY – STEPS TOWARDS A NEW SYSTEM OF INTERNET GOVERNANCE*, Fondation pour l'innovation politique, 01.2017, [online:] http://www.fondapol.org/en/etudes-en/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/.

61 Wright N., *How Artificial Intelligence Will Reshape the Global Order. The Coming Competition Between Digital Authoritarianism and Liberal Democracy*, Foreign Affairs, 10.07.2018.

Tomasz Piekarz

TECHNOLOGIE CYFROWE JAKO ELEMENT POTĘGI MOCARSTW

TECHNOLOGIE CYFROWE, POTĘGA A CYBER POWER

Digitalizacja ściśle wiąże się z wykorzystaniem technologii cyfrowych pozwalających m.in. na swobodną komunikację bez względu na stawiane przez geografię bariery. Z kolei termin technologie cyfrowe określa zbiorczo urządzenia i rozwiązania bazujące na systemie binarnym i transmitujące informacje za pomocą bitów. Są to m.in. urządzenia elektroniczne posiadające półprzewodniki pozwalające rozwiązywać zarówno skomplikowane oraz proste problemy matematyczno-logiczne jak np. komputery i wszystkie urządzenia posiadające mikroprocesory, a także innowacje, które przyczyniły się do masowego przepływu danych zapisywanych w systemie binarnym jak Internet, czy też sieci teleinformatyczne[1].

Potęga jest zagadnieniem, któremu badacze teorii stosunków międzynarodowych poświęcili wiele tomów opracowań formułując równie wiele definicji. Pomimo tego, jest koncepcją „zaskakująco nieuchwytną i trudną do zmierzenia”[2], która w swej wielości definicyjnej odzwierciedla często interesy i wartości osób lub podmiotów ją definiujących. Najpowszechniejsze rozumienie potęgi w naukach politycznych odnosi się do zdolności wpływania na inne podmioty w celu spełnienia przez nie własnej woli. Jednakże, określenie samej potęgi aktorów bez określenia celu jej użycia daje niepełny efekt ponieważ różne cele, w relacji z różnymi aktorami wymagają różnych elementów, w różnej domenie. Dlatego też określanie potęgi danego mocarstwa zawsze zależy od kontekstu jej użycia, (np. militarnego, gospodarczego), wykorzystywanych elementów oraz domeny działania (ląd, woda, powietrze, przestrzeń kosmiczna, czy też cyberprzestrzeń)[3].

Potęga może być badana również pod względem zasobów, relacji i pozycji w strukturach systemu międzynarodowego. Posiadanie zasobów, które mogą być mierzalne jak np. wielkość gospodarki, populacji lub złoża surowców daje badaczom możliwość kwantyfikacji potęgi, a aktorom państwowym możliwość wpływania na zachowanie innych, np. poprzez uzależnienie ich od własnych zasobów surowcowych. Badanie relacji pomiędzy państwami odnosi się szerzej do percepcji zdolności wpływu aktora A na aktora B w ich relacji poprzez analizę przeszłych i teraźniejszych stosunków, zdolności aktora do kształtowania środowiska relacji, umiejętności wykorzystania relacji z danym aktorem i jej manifestacji oraz zdolności do utrzymania relacji w czasie. Z kolei potęga strukturalna odnosi się do wpływu aktora na system międzynarodowy i instytucje oraz normy, które determinują zachowanie państw[4].

Bezprecedensowe tempo rozwoju technologii cyfrowych spowodowało pojawienie się dyskusji o ich wpływie na potęgę państw. Początkowo, debata była zdominowana przez kosmopolityczne podejście i przedstawiała nowe technologie oraz cyberprzestrzeń jako narzędzie emancypacji społeczeństw dzięki ich właściwościom mającym wpływ na szerzenie demokracji, co wyraża m.in. *Deklaracja niepodległości cyberprzestrzeni* Johna Barlowa z 1996 r. Badacze w latach dziewięćdziesiątych XX wieku zwrócili również uwagę na szerszą dystrybucję potęgi cyfrowej na korzyść aktorów niepaństwowych, z kolei stratedzy państwowi z początkiem XXI wieku wprowadzali koncepcje zakładające, że cyberprzestrzeń może być domeną działań wojennych, i za taką została pierwszy raz uznana przez Pentagon w 2011 r. Wydarzenie to było poprzedzone intensywną debatą rozpatrującą zarówno utratę części potęgi przez państwo, jak i możliwe wzmocnienie państwa w nowym obszarze działalności, co zaowocowało w 2009 r. wykuciem terminu potęgi cyfrowej (ang. *Cyber Power*)[5]. W założeniu potęga cyfrowa jest to „zdolność wykorzystania cyberprzestrzeni do tworzenia przewag i wpływania na wydarzenia w innych teatrach operacyjnych i na różne elementy potęgi”[6] tak więc zakłada możliwość otrzymania rezultatów działań zarówno w cyberprzestrzeni, jak i w innych domenach. Z kolei cyberprzestrzeń należy traktować jako unikalną hybrydę infrastruktury fizycznej znajdującej się na lądzie i w przestrzeni kosmicznej oraz sieci wirtualnej[7]. O ile wyróżnienie potęgi cyfrowej jako elementu potęgi państwa jest powszechnie akceptowalne, o tyle część badaczy podkreśla jej brak zdolności do wygrania wojny umieszczając ją niżej w hierarchii od tradycyjnych elementów potęgi[8].

Wraz ze wzrostem zależności od sieci, systemów i zasobów cyfrowych, postępującą konwergencją infrastruktury fizycznej z technologią cyfrową, a także rosnącym znaczeniem danych cyfrowych, w drugiej dekadzie XXI w. należy, wyróżnić technologie cyfrowe, jak i cyberprzestrzeń, jako element i domenę potęgi mocarstw. Jest ona komplementarna wobec tradycyjnych elementów, przynosząc krajom znaczną wartość dodaną na poziomie taktycznym i strategicznym. Wielość cyfrowych technologii, pozwala wśród nich wyodrębnić te o szczególnym znaczeniu geopolitycznym i ekonomicznym. Wśród najistotniejszych warto wyróżnić te, które zakwalifikowane zostały do puli *emerging and disruptive technologies* przez Sojusz Transatlantycki (rozwiązania z zakresu Big Data, Sztuczna Inteligencja, technologie autonomiczne, kosmiczne, hipersoniczne, kwantowe, biotechnologia oraz inżynieria materiałowa[9]), a także wyróżnione przez KE *Key Enabling Technologies* (zaawansowana produkcja, inżynieria materiałowa, technologie nauk przyrodniczych, mikro oraz nanoelektronika i fotonika, Sztuczna Inteligencja, bezpieczeństwo i łączność)[10] oraz advanced technologies (np. IoT, dane przemysłowe, robotyka, druk 3D, *blockchain*, Sztuczna Inteligencja)[11].

TECHNOLOGIE CYFROWE A SOFT, HARD, SMART I CYBER POWER

W opracowaniach opisujących potęgę państw terminy soft, hard i smart power stały się jednym z najpopularniejszych sposobów analizowania tego zagadnienia. Autor koncepcji Joseph S. Nye

wyróżnia trzy metody odpowiadające rodzajom potęg, poprzez które aktor A może skłonić aktora B do spełnienia jego woli. Tak więc, działanie za pomocą przymusu i zapłaty należy do narzędzi hard power, która zakłada wykorzystanie instrumentów i zdolności militarnych oraz ekonomicznych, z kolei skłanianie do działania z wolą aktora A poprzez atrakcyjność jego kultury, wartości, systemu politycznego czy dyplomacje jest domeną soft power. Podczas gdy mechanizmy hard power zakładają stosowanie gróźb użycia siły i wprowadzenia sankcji traktując stosunki między państwami jako grę o sumie zerowej, soft power poprzez perswazje dąży do szukania wspólnego gruntu. Niemniej jednak, sama soft power nie jest w stanie tworzyć efektywnej polityki zagranicznej mocarstwa – oglądane i lubiane przez Kim Dzong Ila filmy z Hollywood nie wpłynęły na program nuklearny Korei Płn.[12], tak jak zamiłowanie do bejsbolu wśród władz i społeczności Wenezueli i Kuby nie wpłynęło na zmianę orientację politycznej tych państw[13]. Dlatego, aby prowadzić efektywną politykę zagraniczną konieczne jest unikalne połączenie dwóch wymiarów potęgi. Takie połączenie, nazwane przez J. S. Nye'a *smart power*, oparte jest na inteligencji kontekstualnej, która pozwala przyjąć odpowiednią taktykę do realizacji danego celu doprowadzając m.in. do zburzenia muru berlińskiego przez mieszkańców miasta, a nie amerykańskie czołgi[14].

Koncepcje hard i soft power są stosowane m.in. do analizy wpływu technologii cyfrowych na potęgę, czego dokonuje sam ich autor J. S. Nye opisując ją jako *cyber power*. Cechą wyróżniającą nową, cyfrową domenę są niskie bariery wejścia (również dla aktorów niepaństwowych) i wiążąca się z tym **szeroka dystrybucja potęgi oraz ograniczony związek z geografią poprzez jej dwuwymiarowość w postaci wirtualnej i fizycznej.** Wirtualny wymiar technologii sprawia, że „przemieszczanie elektronów przez cały świat jest tańsze i szybsze niż przemieszczanie dużych statków na duże odległości”[15]. Niski koszt wejścia i duże możliwości działania w domenie cyberprzestrzeni skutkują zwiększoną obecnością aktorów niepaństwowych oraz małych państw, które odgrywają znacznie większą rolę niż w innych obszarach. W klasycznych domenach projekcji potęgi jedynie nieliczne i najbogatsze państwa mogą utrzymywać flotę zdolną do przemierzania oceanów lub floty myśliwców piątej generacji utrzymując kontrolę nad danym terytorium. Z kolei w cyberprzestrzeni ta zasadność jest ograniczona. O ile istnieją państwa, które rozbudowują zdolności cybernetyczne, o tyle nie można stwierdzić, że któreś posiada dominującą pozycję[16]. Ponadto, niskie bariery prowadzenia działalności powodują, że mniejsze państwa jak np. Korea Północna mogą „uderzać powyżej swojej wagi” prowadząc ataki na państwa i organizacje, na które w innych domenach nie mogłyby sobie pozwolić[17]. Świadczy to również o postrzeganiu przez państwa ataków w cyberprzestrzeni jako obszaru działania hybrydowego poniżej progu wojny. Wiąże się to także z podwójnym zastosowaniem wielu technologii, które stworzone do użytku cywilnego mogą ulec weaponizacji (przystosowaniu do użycia jako broń) i zostać wykorzystane w działaniach hybrydowych. Ponadto, aktorzy wykorzystujący technologie cyfrowe do prowadzenia wrogich działań (ang. *adversarial use of technology* [a]) mają przewagę, gdyż Internet i składowe cyberprzestrzeni, nie były i wciąż nie są stworzone z prymatem zasady bezpieczeństwa (*security by design*, *security by default*), co ogółem sprawia, że cyberprzestrzeń jest dla nich niezwykle atrakcyjnym miejscem do projekcji siły. Dlatego też, jest to domena wykorzystywana przez niepaństwowe grupy i przestępców działających z pobudek finansowych lub ideologicznych (haktywiści). Związki cyberprzestrzeni z geografią również nie pozostają bez wpływu na potęgę państw ponieważ centra danych, światłowody i serwerownie mają fizyczną lokalizację znajdującą się pod jurysdykcją danego rządu. W związku z tym działania o charakterze *soft* i *hard* w domenie cyfrowej mogą być skierowane zarówno wewnętrznie, jak i zewnętrznie, na infrastrukturę krytyczną i jej elementy IT i OT[18].

a Temat wrogich działań prowadzonych w cyberprzestrzeni jest tematem przewodnim CYBERSEC Global 2020 pod hasłem „Together Against Adversarial Internet”, [online:] https://cybersecforum.eu/

TECHNOLOGIE CYFROWE I MILITARNY WYMIAR HARD POWER

Działania militarne oparte na, bądź wspierane przez technologie cyfrowe oraz te prowadzone w cyberprzestrzeni mogą być stosowane zarówno jako odosobnione akty agresji i wrogości w celu przymuszenia aktora B do realizacji woli aktora A, jako element wojny hybrydowej, czy też jako działania towarzyszące wojnie konwencjonalnej mając na celu infrastrukturę cyfrową lub fizyczną przeciwnika.

Technologie cyfrowe stworzyły nową przestrzeń i narzędzia dla przeprowadzania aktów agresji wobec innych państw. Operacją, która zdobyła największy rozgłos i zasłynęła jako pierwsza cyberbroń był Stuxnet robak komputerowy stworzony wspólnie przez USA i Izrael w celu spowolnienia irańskiego programu nuklearnego (więcej informacji o ofensywnych działaniach w cyberprzestrzeni w rozdziale dziesiątym). Irańczycy dostrzegając potencjał cyfrowej broni i domeny wzmocnili inwestycje w rozwój własnych zdolności cybernetycznych oraz rozpoczęli finansowanie wielu grup hakerskich jak Ashiyane czy Cyber Hezbollah[19]. Efektem rozwoju zdolności stały się serie cyberataków na przedsiębiorstwa wydobywcze w Arabii Saudyjskiej i Katarze wielokrotnie w latach 2012, 2014 i 2017. Chociaż Iran oficjalnie się do nich nie przyznaje to eksperci są zgodni co do kraju pochodzenia ataków. Używając wirusa Shamoon zniszczono około 30 000 komputerów firmy Aramco oraz niemalże doprowadzono do wybuchu w elektrowni[20]. Eskalacja napięć w cyberprzestrzeni nastąpiła również w 2020 roku. W kwietniu doszło do poważnych ataków na infrastrukturę wodną Izraela. Obiektem ataku były oczyszczalnie ścieków i przepompownie. W maju zaatakowany został port w Iranie prowadząc do kilkudniowych komplikacji i utrudnień w ruchu[21]. Na przełomie czerwca i lipca, Iran został dotknięty serią pożarów i wybuchów, które ze względu na miejsce wystąpienia natychmiast wywołały podejrzenia służb i obserwatorów. Do wybuchów doszło w elektrowniach, w ośrodku badań, rozwoju i produkcji rakiet oraz centrum medycznym gdzie zginęło 19 osób. Najwięcej spekulacji wywołał jednak pożar w placówce wzbogacającej uran w Natanz, która w 2010 roku była celem ww. wirusa Stuxnet. Pożar uszkodził budynek przemysłowy znajdujący się w pobliżu głównego obiektu kompleksu. Rzecznik Ministerstwa Spraw Zagranicznych Iranu 23 lipca 2020 r. zaprzeczył twierdzeniom, że wydarzenia w kraju były wynikiem cyberataków, jednak z komentarzy ministerstwa wynika, że śledztwo wciąż trwa[22].

Ukraina od początku konfliktu z Rosją rozpoczętego w 2014 roku mierzy się z presją cyberataków będąc „polem bitwy w cybernetycznym wyścigu zbrojeń o globalne wpływy”[23]. Rosyjska armia oraz grupy, uznawane za mające z nią powiązania jak Fancy Bear, Cozy Bear czy Sandworm wykorzystały toczący się konflikt do doskonalenia swoich umiejętności. Przeprowadzone kilkukrotnie udane ataki dotknęły zarówno infrastrukturę wirtualną ukraińskiej Centralnej Komisji Wyborczej w 2014 r., blokując jej sieć oraz stronę internetową, jak i fizyczną uszkadzając część sieci energetycznej, co dwukrotnie doprowadziło w 2015 r. do przerw w dostawie prądu dla około 230 000 Ukraińców, z obwodów czerniowieckiego, iwanofrankiwskiego i kijowskiego, a w 2016 r. ponownie paraliżując część Kijowa. Do największego i najbardziej kosztownego ataku doszło w 2017 r. Rosyjscy hakerzy dzięki połączeniu kodu, który uszkodził ukraiński system energetyczny z istniejącym malware „Petya”, a także podatnością EternalBlue odkrytą przez National Security Agency (NSA) stworzyli nowy malware – „NotPetya”. Dzięki niemu Rosjanie zdobyli dostęp do komputerów ukraińskich przedsiębiorstw użyteczności publicznej, banków, lotnisk i agencji rządowych, trafiając rykoszetem również w międzynarodowe koncerny jak Maersk, FedEx, czy Merck. Koszty ataku zostały oszacowane na około 10 miliardów dolarów[24]. W kontekście wojen hybrydowych warto również zaznaczyć, że technologie cyfrowe umożliwiły także masowe wykorzystanie sieci społecznościowych oraz mediów cyfrowych do prowadzenia wojny informacyjnej[25] (więcej informacji o wojnie informacyjnej w rozdziale trzynastym).

Działania w domenie cyberprzestrzeni towarzyszące wojnie miały miejsce m.in. w 2008 r. Na kilka tygodni przed wkroczeniem Rosjan do Osetii Południowej w sierpniu 2008 r. dokonano ataków DDoS na gruzińskie strony rządowe doprowadzając do przeciążenia serwerów na ponad 24 godziny. Do właściwego ataku doszło wraz z wybuchem wojny. Grupy powiązane z Rosją zdołały doprowadzić do paraliżu informacyjnego, gdyż chwilowo nie działała większość stacji telewizyjnych oraz strony internetowe z gruzińską domeną, z kolei strony rządowe były przez większość trwania konfliktu zablokowane. Ataki dotyczyły jedynie infrastruktury cyfrowej i miały ograniczony zasięg ze względu na niski poziom cyfryzacji Gruzji w 2008 roku[26]. Technologie cyfrowe wpłynęły nie tylko na ustanowienie nowej domeny działań wojennych przez NATO w 2016 roku obok powietrza, morza, lądu i przestrzeni kosmicznej, ale mają również zastosowanie w każdej z pozostałych[27]. Pierwsza wojna w Zatoce Perskiej w 1991 roku stała się kamieniem milowym dla wykorzystania nowych technologii w polu walki prowadząc do rewolucji w prowadzeniu wojen (ang. RMA – revolution in military affairs) za sprawą informatyzacji. Dynamiczna komputeryzacja doprowadziła do powstania precyzyjnych systemów zbrojnych i naprowadzania, zintegrowanych systemów dowodzenia, które poprzez analizę danych pozwalają decydentom na prowadzenie symultanicznych i szybkich działań połączonych rodzajów sił zbrojnych[28] również z użyciem broni autonomicznej. Technologie cyfrowe umożliwiły powstanie m.in. systemów C4ISR (ang. *Command*, *Control*, *Communications*, *Computers*, *Intelligence*, *Surveillance*, *Reconnaissance*) używanych we współczesnych operacjach zbrojnych, które pozwalają na zdobycie dominacji w zakresie świadomości sytuacyjnej na polu walki i podejmowanie decyzji wpływających na bitwę w czasie rzeczywistym[29]. Z kolei postęp technologiczny w zakresie systemów satelitarnych i zdobywania danych wywiadowczych wzmocnił dążenia mocarstw do posiadania broni precyzyjnego rażenia mogącej zniszczyć satelity przeciwnika. Takie zdolności obecnie posiadają Chiny, Indie, Rosja i Stany Zjednoczone[30].

Przytoczone powyżej zdarzenia mają wspólną cechę, którą jest dążenie przez aktora A do wymuszenia zmiany zachowania aktora B. Pokazują, że technologie cyfrowe konstytuują nowy obszar działań militarnych, a także przenikają pozostałe domeny poprzez cyfrowe innowacje militarne. Technologia cyfrowa jest wszechobecna i pozwala na zintegrowanie działań wojskowych w powietrzu, na lądzie i morzu, tworząc bezprecedensowe zdolności wywiadowcze oraz systemy dowodzenia dające dostęp do informacji w czasie rzeczywistym. Bez wątpienia technologie cyfrowe zmieniły przebieg działań wojennych. Niemniej jednak, operacje cybernetyczne państw mające na celu zniszczenie danych lub sabotaż to jedynie około 7% odnotowanych incydentów, podczas gdy odnotowane przypadki szpiegostwa stanowią około 82%[31].

TECHNOLOGIE CYFROWE I EKONOMICZNY WYMIAR HARD I SOFT POWER

Posiadanie rozwiniętej i efektywnej gospodarki spełniającej stawiane przed nią cele, wpływa podobnie jak technologie cyfrowe, na inne rodzaje potęgi pozwalając państwom na odpowiednie finansowanie jej wybranych elementów mających zrealizować dane cele strategiczne. Tym samym potęga ekonomiczna katalizuje ogólną potęgę mocarstw i w obecnym systemie międzynarodowym mocniej wpływa na ich pozycję niż element militarny. Potęga ekonomiczna składa się z kilku połączonych i wzajemnie na siebie oddziałowujących czynników opisanych poniżej. Pierwszym z czynników jest relatywny rozmiar gospodarki, który odnosi się do obecnej i przyszłej jej wielkości oraz wielkości rynku, do którego można odmówić lub utrudnić dostęp aktorom w celu wymuszenia zmiany zachowania. Drugim z czynników jest zdolność państwa lub grupy państw do współpracy międzynarodowej w ramach umów handlowych lub innych deklaratywnych działań, która obrazuje oczekiwany wzrost gospodarki. Trzeci czynnik zawierający aspekty intelektualne i reputacji odnosi się do gospodarki jako soft power mocarstwa, jego zdolności do wpływania i perswazji na innych aktorów[32].

Wpływ technologii cyfrowych na gospodarkę jest rewolucyjny, o czym świadczy fakt, że są one motorem napędowym czwartej rewolucji przemysłowej, której fundamentem jest Internet, taniejąca i dostępniejsza moc obliczeniowa, olbrzymie zasoby danych cyfrowych i masowe ich przetwarzanie, a także gigantyczne możliwości komunikacji i przesyłu danych z małymi opóźnieniami poprzez sieć 5G, która przyczyni się m.in. do dynamicznego rozwoju Internetu Rzeczy i automatyzacji produkcji przemysłowej. Cyfryzacja katalizuje również rozwój w pozostałych segmentach gospodarki, które uczestniczą w rewolucji – m.in. pojazdy autonomiczne, druk 3D, czy też biomedycyna i nowoczesne urządzenia diagnostyczne[33]. Co więcej, rewolucja przebiega w bezprecedensowym tempie tworząc nowe rynki (np. wirtualnej rzeczywistości (VR), Sztucznej Inteligencji) i zawody jednocześnie zastępując inne[34]. O jej tempie może świadczyć skala transferu danych przez IP, która w 1992 r. wynosiła 100 gigabajtów (GB) na dobę, w 2017 r. więcej niż 45 000 GB na sekundę i według prognoz w 2022 r. osiągnie pułap 150 700 GB na sekundę, a to dopiero początek rewolucji[35].

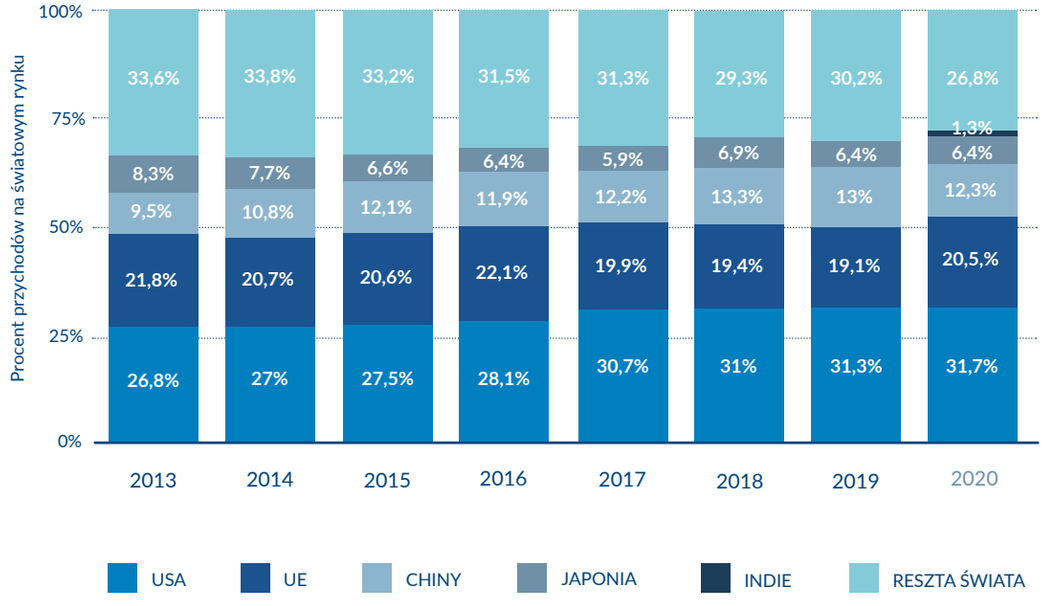
Analizując geografię cyfrowej gospodarki wyłania się obraz bipolarnego świata, w którym dominują Stany Zjednoczone i Chiny. Sumarycznie kraje te w połowie 2019 r. odpowiadały za 75% patentów związanych z technologią *blockchain*, 50% globalnych wydatków na technologię IoT, tworzyły ponad 75% światowego rynku publicznego *cloud computing* oraz odpowiadały za 90% kapitalizacji rynkowej siedemdziesięciu największych platform cyfrowych, podczas gdy europejski udział w rynku platform to jedynie 4%[36]. Należy zaznaczyć, że pomimo przewagi dwóch państw w ww. technologiach, udział UE w wytwarzaniu rozwiązań technologii 5G, która będzie motorem napędowym rewolucji cyfrowej, jest dominujący. Świadczy o tym fakt, że dwie na trzy firmy posiadające całościowe rozwiązania w zakresie budowy sieci 5G pochodzą z państw wspólnoty[37]. Ponadto, UE posiada około 20% udziałów w globalnym rynku ICT, który konstytuują głównie zagraniczni inwestorzy i kilku europejskich czempionów (rysunek nr 1). Ze względu na brak powszechnie przyjętej definicji gospodarki cyfrowej, ONZ poprzez uśrednienie badań szacuje, że odpowiada ona za 4,5 do 15,5% światowego PKB – USA i ChRL odpowiadają za niemalże 40% światowej wartości dodanej ICT, a sam udział sektora technologii cyfrowych w gospodarkach państw jest największy w Tajwanie, Irlandii i Malezji. Z kolei eksport usług sektora ICT oraz innych, dostarczanych cyfrowo stanowił w 2018 r. już połowę światowego eksportu usług[38].

Istniejące badania wskazują na korelację wzrostu gospodarczego ze wzrostem penetracji gospodarek przez liczbę użytkowników Internetu. Niemniej jednak, analitykom nie udało się dotychczas stwierdzić, który czynnik jest determinantą, innymi słowy, czy wzrost poziomu dostępności Internetu spowodowany jest wzrostem gospodarczym, czy wzrost gospodarczy powoduje wzrost penetracji sieci internetowej. Analogiczne wnioski dotyczą analizy rozwoju sektora ICT i wzrostu produktywności. Ponadto, korelacje te różnią się w różnych państwach, np. silniejsze są w krajach rozwijających się niż w krajach rozwiniętych[39]. Pomimo niezidentyfikowania determinanty korelacji, przyjmuje się poprzez konsensus, że innowacje są motorem napędowym wzrostu gospodarczego, którego główna miara, jaką jest PKB, ma pewne ograniczenia, np. mierzy zyski platform ze sprzedanych reklam, jednak nie mierzy wartości dodanej wytworzonej przez konsumentów platformy za darmo. Ponadto, innowacje odzwierciedlane są w PKB dopiero po „dostosowaniu makroekonomii"[40], gdyż na przestrzeni wieków rewolucyjne technologie, takie jak elektryczność, a obecnie Internet z początku prowadziły do upadku wielu przedsiębiorstw niedostosowanych do nowej rzeczywistości, przynosząc jednak równocześnie wiele korzystnych, lecz niemierzalnych efektów dla ogółu społeczeństwa[41].

Kluczowym zasobem gospodarki cyfrowej są dane cyfrowe, które pozwalają na tworzenie wartości dodanej. Kontrola nad nimi jest strategicznie istotna dla państwa z punktu widzenia bezpieczeństwa i właściwej alokacji hard czy soft power,

dostarczając m.in. nieocenione dane wywiadowcze. Ponadto, „w każdym łańcuchu wartości, umiejętność gromadzenia, przechowywania, analizy i transformacji danych niesie ze sobą dodaną potęgę i przewagę konkurencyjną"[42]. W wymiarze ekonomicznym, dane są rdzeniem wszystkich technologii cyfrowych przyszłości (m.in. *AI*, *IoT*, *blockchain*, *cloud*), a kontrolę nad nimi sprawują głównie globalne platformy cyfrowe, które posiadają najlepsze zdolność do ich wykorzystania i wygenerowania wartości dodanej powodując tym samym dalszą konsolidację i koncentrację gospodarki cyfrowej (więcej o znaczeniu danych cyfrowych w rozdziale piątym). W związku z tym, w globalnym łańcuchu wartości danych większość państw jest zależy od globalnych firm technologicznych i platform internetowych. O ekonomicznej dominacji USA w zakresie przetwarzania danych może świadczyć pozycja rynkowa Google – 90% rynku wyszukiwarek Internetowych[43], Microsoft – 78% rynku systemów operacyjnych[44], Facebook – 70% rynku mediów społecznościowych, Amazon – niemalże 40% rynku detalicznego handlu elektronicznego, Amazon Web Services – niemalże 40% rynku usług chmury komputerowej. Z kolei firmy chińskie jak WeChat czy Alibaba pomimo posiadania imponującej liczby użytkowników skupione są głównie na rynku wewnętrznym, posiadając mniejszy udział w globalnym rynku ICT[45], który kształtuje się następująco:

RYSUNEK 1.
UDZIAŁ PAŃSTW W GLOBALNYM RYNKU ICT OD 2013 DO 2020 ROKU.



Źródło: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/

Dominacja Stanów Zjednoczonych na globalnym rynku ICT sprawia, że mogą nie tylko stosować narzędzia utrudniające dostęp do rynku w celu wymuszenia zmiany zachowania innego aktora, ale również wpływać na innych aktorów w celu przyjęcia przez nich paralelnych narzędzi. Przykładem może być przypadek Huawei, któremu ze względu na kwestie bezpieczeństwa USA nie tylko uniemożliwiło działanie na rynku amerykańskim[46] i efektywnie wpłynęło na podobne decyzje niektórych sojuszników[47], ale również korzystanie z komponentów amerykańskich firm co poważnie wpłynęło na kondycję firmy[48]. Stosując zarówno bariery dostępu do rynku jak i wykorzystując zależność technologiczną (która również jest elementem potęgi mocarstwa podobnie jak zależność od surowców energetycznych) USA wykorzystuje potęgę ekonomiczną i rozwinięty sektor ICT do projekcji własnej potęgi wobec działań innego mocarstwa.

TECHNOLOGIE CYFROWE A SOFT POWER

Waga soft power po zakończeniu zimnej wojny staje się sukcesywnie większa przesuwając środek ciężkości z hard power. Przyczyniła się do tego w znacznej mierze cyfrowa rewolucja, która stworzyła nową przestrzeń dając nowe narzędzia aktorom. Tak więc, technologie cyfrowe wpływają na soft power paralelnie jak w przypadku hard power – tworzą nową przestrzeń działania państw, ale również nowe metody i narzędzia do kształtowania soft power przenikając niemalże każdą sferę życia publicznego. Dzięki temu globalna dystrybucja soft power nie tylko zmienia się na korzyść państw azjatyckich, ale również aktorów niepaństwowych. Z kolei wielowymiarowe, kompleksowe i współzależne stosunki międzypaństwowe w XXI wieku wymusiły na państwach wzmocnienie roli miękkich narzędzi do realizacji własnych celów politycznych[49].

Joseph Nye, wspomniany już twórca koncepcji soft power odwołuje się do indeksu The Soft Power 30, stworzonego przez Centrum Dyplomacji Publicznej Uniwersytetu Południowej Kalifornii oraz firmę konsultingową Portland, w rozmowie udostępnionej jako podcast, której gospodarzem był, *nomen omen* duński Tech Ambassador Casper Klynge[b] – co samo w sobie jest przykładem użycia technologii cyfrowych do kreacji soft power[50]. Indeks w oparciu o przyjętą metodologię kwantyfikuje soft power państw i prowadzi ich ranking łącząc dane obiektywne (65% wyniku) i subiektywne (35% wyniku) poprzez badanie opinii respondentów. Do danych obiektywnych należą kategorię: przedsiębiorczość, kultura, cyfryzacja, rząd, zaangażowanie i edukacja. Z kolei do każdej kategorii przyporządkowane są mierzalne dane statystyczne. Tak więc komponent cyfrowy soft power (którego istotność rośnie w porównaniu do lat poprzednich) mierzy jak technologie cyfrowe przenikają życie społeczne, efektywność publicznych usług online, dostępność i jakość połączenia z Internetem oraz skalę jego użytkowania w dyplomacji i codziennym życiu społeczeństwa. Łączny wynik w tej kategorii składa się na 13,1% wpływu danych obiektywnych. Indeks mierzy również opinię o produktach technologicznych wytwarzanych w danych państwach, która z kolei wpływa na 8,3% danych subiektywnych[51]. Ranking 10 najpotężniejszych państw w obiektywnej kategorii cyfrowej wygląda następująco:

1. Stany Zjednoczone,
2. Kanada,
3. Wielka Brytania,
4. Francja,
5. Korea Południowa,
6. Szwajcaria,
7. Japonia,
8. Singapur,
9. Szwecja,
10. Nowa Zelandia.

Stany Zjednoczone zajmują pierwsze miejsce w rankingu ze względu na globalną dominację amerykańskich gigantów technologicznych jak

b *Tech Ambassador* Królestwa Danii, sierpień 2017 – marzec 2020. Obecnie European Government Affairs, Microsoft.

i bezprecedensową aktywność prezydenta Trumpa w mediach społecznościowych. Kanada, Wielka Brytania i Francja zawdzięczają swój wynik rozwiniętym publicznym usługom cyfrowym oraz miarom dyplomacji cyfrowej, z kolei wynik Korei Południowej opiera się na posiadaniu najszybszego połączenia internetowego na świecie[52]. Polska w kategorii cyfrowej zajmuje 20 miejsce na świecie i jest to najlepszy wynik spośród wszystkich komponentów naszego kraju badanych w Indeksie[53].

Technologie cyfrowe zrewolucjonizowały tradycyjne metody dyplomacji publicznej i komunikacji państwa. Zmieniły się nie tylko kanały wysyłania komunikatu, ale również sposób dobierania komunikatów do określonych grup społecznych, który dzięki rozwiązaniom „Big Data i SI" jest zautomatyzowany. Cyberprzestrzeń stała się nową płaszczyzną do kreowania soft power. Poprzez użycie Internetu państwa mogą oddziaływać na społeczeństwa w innych częściach świata mając na celu kreowanie atrakcyjności swojej lub danego aktora w oczach innych jednostek i państw, a także mogą wpływać na własne społeczeństwo i jego nastawienie wobec państw trzecich.

Rewolucja cyfrowa to również wyzwanie dla państw w kontekście regulacji prawnych i ich dostosowania do funkcjonowania w nowej rzeczywistości, która szczególnie naraża prywatność użytkowników[54]. Warto odnotować, że wyzwanie to zostało w znacznej mierze zagospodarowane przez UE, która poprzez swoje rozwiązania prawne w zakresie nowych technologii, cyberbezpieczeństwa, czy prywatności, często wyprzedzające inne kraje, wytycza im drogę i wskazuje globalnym firmom kierunki dostosowania się do nich – co samo w sobie jest współczesnym elementem soft power Unii, który przyjmuje formę normatywną i regulacyjną (ang. *regulatory*, *normative power*)[55]. Należy zauważyć, że wykorzystanie przez państwa nowych mediów w kształtowaniu stosunków międzynarodowych ma niekiedy formy działań dezinformacyjnych i interferowania w kampanie wyborcze toczące się w państwach o innej orientacji geopolitycznej. Za przykład może posłużyć rosyjskie zaangażowanie podczas kampanii przed referendum o wyjściu Wielkiej Brytanii z UE[56].Cyberprzestrzeń stała się również miejscem, w którym poszczególne krają starają się wprowadzać rozwiązania ograniczające przepływ informacji i wolność słowa. O ile państwa demokratyczne nie ograniczają dostępności witryn i treści tworzonych przez użytkowników Internetu, o tyle państwa autorytarne często uciekają się do prób jego cenzurowania. Zależność ta sprawia, że państwa niedemokratyczne chętnie współpracują nad rozwiązaniami mającymi na celu cenzurę treści zamieszczonych w sieci internetowej[57].

Technologie cyfrowe wzmacniają soft power państw także w zakresie tworzenia ich wizerunku pośród społeczności międzynarodowej dzięki użyciu nowych, globalnych mediów społecznościowych. Cyfryzacja ponownie wspomaga państwa w kreowaniu potęgi poprzez nowe kanały, które mogą służyć do promowania kultury, walorów turystycznych, czy też systemu rządu danego państwa starając się jednocześnie zdobyć przychylność obywateli innych państw. Ponadto, rozwinięty sektor nowych technologii wpływa na zwiększenie soft power państwa w innych segmentach. Może np. wspierać eksport dóbr kulturowych dystrybuując je w sposób cyfrowy, czy też udostępniając swoje technologie dla szkół w innych państwach lub tworząc nowoczesne centra danych wpływające na rozwój gospodarki danego państwa.

Technologie cyfrowe nie odgrywają jednak w soft power tak dużego znaczenia jak w elementach hard power. O ile wykorzystuje się je do promowania wizerunku danego kraju i wpływają na jego percepcję, o tyle mają ograniczony wpływ na kulturę i historię. Należy zaznaczyć, że cyfryzacja tych dwóch nieodłącznych elementów miękkiej potęgi przyczynia się znacznie do ich rozpowszechniania, jednak nie zmienia natury historycznych wydarzeń i dóbr kultury. „Budowa i utrzymanie zaufania oraz soft power wymaga czasu"[58], który w skali historii istniejących państw nie jest przychylny dla technologii cyfrowych będących wciąż relatywną nowością. Niemniej jednak, tempo zmian

technologicznych, procesów regulacyjnych i działań mających na celu budowanie zaufania i bezpiecznego ekosystemu technologii cyfrowych sprawia, że historia znacznie „przyśpiesza", a dekada w skali rozwoju technologii przynosi diametralne zmiany.

TECHNOLOGIE CYFROWE – REWOLUCJA W STOSUNKACH MIĘDZYNARODOWYCH

Do maja 2019 r. żyliśmy w przekonaniu, że „połączone siły globalizacji i technologii służą spajaniu krajów, a nie ich rozdzieraniu"[59]. Jednak cezura (16 maja 2019) związana z umieszczeniem chińskiego giganta technologicznego Huawei na czarnej liście amerykańskiego Departamentu Handlu, a następnie coraz bardziej pogłębiający się kryzys relacji amerykańsko-chińskich oraz konsekwencje pandemii COVID-19, doprowadziły nas do momentu, w którym możemy postawić tezę, że rozrywanie cyfrowych łańcuchów dostaw i podział Internetu (*Splinternet*), są bardziej prawdopodobne niż kiedykolwiek wcześniej. **W procesie budowy potęgi element technologii cyfrowych jest nowym polem, które będąc jednocześnie jej katalizatorem może dać przewagę państwom, które tę zależność rozumieją.**

Bez wątpienia, technologie cyfrowe są przełomem dla stosunków międzynarodowych i elementem, który będzie wciąż zyskiwał coraz większe znaczenie. Świadczyć o tym mogą opisywane w dalszych rozdziałach strategiczne działania Chińskiej Republiki Ludowej pod tytułem *Made in China 2025*, czy też amerykańska inicjatywa *Clean Network*, strategia UE „Europa na miarę ery cyfrowej", czy też strategia technologiczna, którą tworzy NATO.

Z pewnością, stosunki międzynarodowe oraz dystrybucja potęgi i metody projekcji siły ulegają i ulegną znacznej zmianie poprzez wpływ technologii cyfrowych. Nowy element potęgi mocarstw katalizuje każdy z jej dotychczasowych wymiarów oraz tworzy nową, unikalną przestrzeń do realizacji celów zarówno hard jak i soft power. Jednocześnie zmianie ulega dystrybucja potęgi. W siłę rosną nie tylko organizacje i grupy niepaństwowe, dla których istotny jest niski próg wejścia do cyberprzestrzeni, ale również dostawcy technologii. Pandemia COVID-19 pokazała, jak kluczowe dla utrzymania ciągłości życia gospodarczego i społecznego są rozwiązania dostarczane przez globalne firmy technologiczne.

J. S. Nye w 2010 roku pisał, że „największe mocarstwa prawdopodobnie nie będą w stanie zdominować tej domeny, tak jak morze czy powietrze"[60]. Dekadę po opublikowaniu tych słów, największe mocarstwa dostrzegając wartość jaką niosą technologie cyfrowe ścigają się o technologiczną supremację, dążą do budowy niezależności cyfrowej, niezależnych sieci internetowych, rozwijają wojska cybernetyczne i prowadzą wojnę informacyjną będąc świadomym, że nowe technologie mogą dać im przewagę nad innymi aktorami zarówno w domenie, którą tworzą, jak i zwiększając ich hard oraz soft power.

PRZYPISY

1 *Digital Technology*, Dictionary of American History, Encyclopedia.com, 2020, [online:] https://www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/digital-technology.

2 Nye J. S., *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010, s. 2.

3 Tamże, s. 2.

4 Hart J. A., *Information and Communications Technologies and Power*, w: *Cyberspace and Global Affairs*, Costigan S., Perry J., (red.) Ashgate Publishing, 2012, s. 207-211.

5 Dunn Cavelty M., *Europe's cyber-power*, European Politics and Society, 2018, 19(3), s. 304-307.

6 Kuehl D. T., *From Cyberspace to Cyberpower: Defining the Problem*, [w:] Kramer F. D., Starr S., Wentz L. K. (red.), *Cyberpower and National Security*, National Defense UP, Potomac Books, Washington, D.C., 2009, s. 38.

7 Nye, *Cyber Power*, op. cit., s. 3-4.

8 Dunn Cavelty M., *Europe's cyber-power*, op. cit., s. 307.

9 Reding D. F., Eaton J., *Science & Technology Trends 2020-2040. Exploring the S&T Edge*, NATO Science & Technology Organization, 2020, s. vii, [online:] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

10 *Key enabling technologies policy*, European Commission, 2020, [online:] https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-innovation/key-enabling-technologies_en.

11 *Internal Market, Industry, Entrepreneurship and SMEs*, European Commission, 2020, [online:] https://ec.europa.eu/growth/industry/policy/advanced-technologies_en.

12 Nye J. S., *Get Smart: Combining Hard and Soft* Power, Foreign Affairs, 2009, 88(4), s. 160-161.

13 Arsenault C., *'Baseball diplomacy' strikes out in Venezuela*, AL JAZEERA, 2013, [online:] https://www.aljazeera.com/in-depth/features/2013/03/201331013310778232.html.

14 Nye, *Get Smart: Combining Hard and Soft Power*, op. cit., s. 160-163.

15 Nye, *Cyber Power*, op. cit., s. 4.

16 Tamże, s. 3-4.

17 Perlroth N., Sanger D. E., *U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing*, The New York Times, 2020, [online:] https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html.

18 Nye, *Cyber Power*, op. cit., s. 4-6.

19 Hodgson Q. E., Ma L., Marcinek K., Schwindt K., *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*, RAND Corporation, 2019, s. 23-24.

20 Tamże, s. 24-27.

21 Mehdi S. Z., *Iran group claim attacks on 28 Israeli railway stations*, Anadolu Agency, 2020, [online:] https://www.aa.com.tr/en/middle-east/iran-group-claim-attacks-on-28-israeli-railway-stations/1927997 .

22 Düz Z. N., *Iran: Recent fires not caused by cyberattacks*, Anadolu Agency, 2020, [online:] https://www.aa.com.tr/en/middle-east/iran-recent-fires-not-caused-by-cyberattacks/1919842#.

23 Laurens Cerulus, *How Ukraine became a test bed for cyberweaponry*, POLITICO, 2019, [online:] https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

24 Tamże.

25 *Social Media as a Tool of Hybrid Warfare*, NATO Strategic Communications Centre of Excellence, 2016, s. 40-41 [online:] https://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

26 Markoff J., *Before the Gunfire, Cyberattacks*, The New York Times, 2008, [online:] https://www.nytimes.com/2008/08/13/technology/13cyber.html.

27 NATO, *Cyber defence*, NATO, 2020, [online:] https://www.nato.int/cps/en/natohq/topics_78170.htm.

28 Davis N., *An Information-Based Revolution in Military Affairs*, Strategic Review, 1996, 24(1), U.S. Strategic Institute, s. 83-86.

29 Ferris J., *Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?*, Intelligence & National Security, 2004, 19(2), s. 199.

30 Ziemnicki P., *Indie zestrzeliły satelitę*, Space24, 2019, [online:] https://www.space24.pl/indie-zestrzelily-satelite.

31 Tamże, s. 3.

32 Němečková T., *Morocco as emerging regional economic power?*, The Journal of North African Studies, 2019, s. 4-6.

33 Gracel J., *Czwarta rewolucja przemysłowa: zmiana już tu jest*, Harvard Business Review Polska, [online:] https://www.ican.pl/b/czwarta-rewolucja-przemyslowa-zmiana-juz-tu-jest-1/2/OmImRGYW.

34 Klaus Schwab, *The Fourth Industrial Revolution What It Means and How to Respond*, Foreign Affairs, 2015, [online:] https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

35 United Nations Conference on Trade and Development, *Digital Economy Report 2019. Value Creation and Capture: Implications For Developing Countries*, United Nations, 2019, s. 1.

36 Tamże, s. 3-7.

37 Bellamy D., *EU insists European companies could replace Huawei in 5G network*, Euronews, 2020, [online:] https://www.euronews.com/2020/07/25/eu-insists-european-companies-could-replace-huawei-in-5g-network.

38 United Nations Conference on Trade and Development, *Digital Economy Report 2019. Value Creation and Capture: Implications For Developing Countries*, op. cit., s. 3-7.

39 Hernandez K., Faith B., Martín P. P., Ramalingam B., *The Impact of Digital Technology on Economic Growth and Productivity, and its Implications for Employment and Equality: An Evidence Review*, IDS Evidence Report 207, IDS, 2016, s. 36.

40 O'Sullivan A., *How Technology Affects Economic Growth And Why It Matters for Policymakers*, The Bridge, Mercatus Center George Mason University, 2019, [online:] https://www.mercatus.org/bridge/commentary/how-technology-affects-economic-growth.

41 Tamże.

42 United Nations Conference on Trade and Development, *Digital Economy Report 2019. Value Creation and Capture: Implications For Developing Countries*, op. cit., s. 7.

43 Tamże, s. 6-7.

44 *Global market share held by operating systems for desktop PCs, from January 2013 to January 2020*, Statista, 2020 [online:] https://www.statista.com/statistics/218089/global-market-share-of-windows-7/.

45 United Nations Conference on Trade and Development, *Digital Economy Report 2019. Value Creation and Capture: Implications For Developing Countries*, op. cit., s. 6-7.

46 Keane S., *Huawei ban timeline: US companies allowed to work with Huawei on 5G standards*, c|net, 2020, [online:] https://www.cnet.com/news/huawei-ban-full-timeline-us-restrictions-china-trump-executive-order-security-threat-5g-commerce/.

47 Buchholz K., *Which Countries Have Banned Huawei?*, Statista, 2020, [online:] https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/#:~:text=As of December 12%2C 2019,new network to 35 percent.

48 Hille K., *Huawei says new US sanctions put its survival at stake*, Financial Times, 2020, [online:] https://www.ft.com/content/3c532149-94b2-4023-82e0-b51190dc2c46.

49 McClory J., *The soft power 30. A Global Ranking of Soft Power 2017*, Portland, USC Center on Public Diplomacy, 2017, s. 10, [online:] https://softpower30.com/wp-content/uploads/2017/07/The-Soft-Power-30-Report-2017-Web-1.pdf.

50 Klynge C., Nye J. S., *Episode 18 – Joseph Nye*, TechPlomacy Talk podcast, 2019.

51 McClory J., *The soft power 30. A Global Ranking of Soft Power 2019*, Portland, USC Center on Public Diplomacy, 2019, s. 27-34, [online:] https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf.

52 Tamże, s. 60-62.

53 *The Soft Power* 30, Portland, USC Center on Public Diplomacy, 2019, [online:] https://softpower30.com/?country_years=2019&sort_by=digital.

54 Wang J., *Public diplomacy and our digital future*, [w:] Jonathan McClory (red.), *The soft power 30. A Global Ranking of Soft Power 2019*, USC Center on Public Diplomacy, Portland, 2019, s. 75-78, [online:] https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf.

55 Hobbs C., *The EU as a digital regulatory superpower: Implications for the United States*, European Council on Foreign Relations, 2019, [online:] https://www.ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u#:~:text=The US and the EU,and levying landmark antitrust fines.

56 Field M., Wright M., *Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals*, The Telegraph, 2018, [online:] https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/.

57 Morgan R., *Russia and China to sign internet censorship treaty*, American Military News, 2019, [online:] https://americanmilitarynews.com/2019/10/russia-and-china-to-sign-internet-censorship-treaty/.

58 Brown K., *Face-time: Building trust in international affairs through exchanges*, *w: The soft power 30. A Global Ranking of Soft Power 2019*, [w:] Jonathan McClory (red.), USC Center on Public Diplomacy, Portland, 2019, s. 107, [online:] https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf.

59 McClory J., *The soft power 30. A Global Ranking of Soft Power 2018*, Portland, USC Center on Public Diplomacy, 2018, s. 23, [online:] https://softpower30.com/wp-content/uploads/2018/07/The-Soft-Power-30-Report-2018.pdf.

60 Nye, *Cyber Power*, op. cit., s. 19.

Barbara Sztokfisz

CYBERDYPLOMACJA – NARZĘDZIE BUDOWANIA CYFROWEGO POKOJU

WPROWADZENIE

Od zarania dziejów narody komunikują się ze sobą z zamiarem osiągnięcia pożądanych celów politycznych, ekonomicznych czy społecznych. Dyplomacja, stanowiąc jedną z najstarszych dziedzin stosunków międzynarodowych, ewoluuje wraz z rozwojem gospodarczym, postępem technologicznym oraz zmieniającymi się przewagami konkurencyjnymi funkcjonujących na arenie międzynarodowej podmiotów. W miarę wzrostu roli cyfryzacji w sferze gospodarczej oraz społecznej, wzmacnianie zaufania, bezpieczeństwa i stabilności w cyberprzestrzeni ma kluczowe znaczenie dla zapewnienia wszystkim interesariuszom możliwości czerpania korzyści z dobrodziejstw najnowszych technologii. Wychodząc naprzeciw wyzwaniom związanym ze złożonością świata cyfrowego, wiele organizacji o charakterze globalnym i regionalnym, a także podmiotów pozapaństwowych jest obecnie aktywnie zaangażowanych w promowanie otwartej, bezpiecznej oraz stabilnej cyberprzestrzeni.

CYBERDYPLOMACJA – POJĘCIE I ZNACZENIE WE WSPÓŁCZESNYCH STOSUNKACH MIĘDZYNARODOWYCH

W tradycyjnym rozumieniu dyplomacja to „działalność władz państwa i ich zagranicznych przedstawicieli w ochronie i realizacji jego interesów zewnętrznych w sposób pokojowy”[1]. W tym znaczeniu sztuka dyplomacji to inteligentne unikanie wojny oraz dążenie do utrwalania pokoju w stosunkach międzynarodowych. Wiek XX przyniósł istotne zmiany funkcjonalne oraz prawne w postaci

kodyfikacji prawa dyplomatycznego[a], jednak podstawowe zadania dyplomacji wydają się aktualne i niezmienne od setek lat. Współczesną dyplomację charakteryzuje między innymi wielostronny charakter oraz rosnąca liczba zaangażowanych w nią podmiotów[2]. Kompetencje, na które niegdyś państwo posiadało monopol, takie jak uczestnictwo w polityce międzynarodowej czy kontrola transnarodowej komunikacji, są obecnie w gestii znacznie szerszego grona aktorów[3]. Jednym z największych wyzwań dla współczesnej dyplomacji jest gwałtowny postęp technologiczny oraz zmieniające się formy komunikacji. Już w XIX wieku, kiedy spopularyzowano użycie telegrafu, Lord Palmerston[b], otrzymując po raz pierwszy wiadomość tego typu, krzyknął: „Mój Boże! To koniec dyplomacji!"[4]. Nic jednak nie wskazuje, aby jego obawy miały się spełnić. Dyplomacja rozwija się bardzo dynamicznie, państwa oraz organizacje międzynarodowe zdają się rozumieć zmieniający się świat i swoimi działaniami odpowiednio reagują.

Cyberdyplomacja stanowi relatywnie nowy wymiar stosunków międzynarodowych. Można ją zdefiniować jako „wykorzystanie funkcji i zasobów dyplomatycznych w celu zabezpieczenia narodowych interesów w cyberprzestrzeni"[5] lub jako „zbiór praktyk dyplomatycznych związanych z szeroko pojętym zarządzaniem cyberprzestrzeni"[6]. W związku z możliwością prowadzenia w przestrzeni cyfrowej działań mających bezpośredni wpływ na bezpieczeństwo narodowe cyberprzestrzeń stała się ważnym obszarem o charakterze politycznym, której kształt często nadają rozbieżne interesy, normy oraz wartości. Ów proces upolitycznienia cyberprzestrzeni sprawia, że dyplomaci odgrywają bardzo istotną rolę w procesie analizy oraz mediacji sporów z nią związanych. Podmiotami krajowymi odpowiedzialnymi za ten obszar są zwykle ministerstwa spraw zagranicznych. W ich ramach często funkcjonuje specjalne stanowisko Koordynatora lub Ambasadora właściwego ds. cyberdyplomacji (w krajach regionu Trójmorza takie stanowisko zostało utworzone między innymi w Estonii[c] oraz w Polsce[7]). Istotne jest odróżnienie tego pojęcia od e-dyplomacji oraz dyplomacji cyfrowej (ang. *e-diplomacy*, *digital diplomacy*), które często mylnie bywają używane naprzemiennie. Dyplomacja cyfrowa oraz e-dyplomacja skupiają się głównie na wpływie nowych technologii, zwłaszcza form komunikacji, na narzędzia oraz metody działań dyplomatycznych. Cyberdyplomacja (ang. *cyberdiplomacy*) natomiast obejmuje zagadnienia rozwiązywania konfliktów, negocjowania umów oraz definiowania polityk dotyczących cyberprzestrzeni[8].

Narzędzia technologiczne wpływają współcześnie na funkcjonowanie wszystkich sektorów gospodarek, a cyfryzacja stanowi priorytet wielu agend politycznych zarówno na poziomie lokalnym, regionalnym, jak i globalnym. Lecz oprócz korzyści, jakie niosą te procesy, dostrzegalne są kwestie takie jak brak inkluzywności w dostępie do nowych technologii (tzw. wykluczenie cyfrowe) czy też wrogie działania w cyberprzestrzeni podejmowane przez podmioty państwowe oraz pozapaństwowe niekiedy nakierowane na krytyczne dla gospodarek obszary – sektor energetyczny, transportowy, służbę zdrowia czy usługi publiczne (w tym systemy wyborcze). Do głównych przyczyn zwiększającego się znaczenia cyberdyplomacji należy przede wszystkim globalny charakter cyberprzestrzeni, która nie zna granic narodowych. W tym znaczeniu jest ona często porównywana do innych dóbr wspólnych takich jak wody międzynarodowe, przestrzeń powietrzna oraz kosmiczna. W związku z tym, w celu maksymalizacji korzyści związanych z równym dostępem do owego zasobu, a także w celu minimalizacji konfliktów, potrzebne są zasady oraz reguły obowiązujące wszystkich, stanowiące wynik negocjacji dyplomatycznych. Pomimo twierdzeń, że prawo międzynarodowe ma zastosowanie również do cyberprzestrzeni, wciąż toczy się dyskusja, w jaki sposób należy je stosować[9]. Cyberprzestrzeń charakteryzuje wiele złożoności, które utrudniają dojście do międzynarodowego konsensusu. Po pierwsze, największe światowe gospodarki i mocarstwa różnią się w swoim podejściu, promując konkurencyjne interesy i wartości. Po drugie, istnieją trudności o charakterze technicznym związane z ustalaniem źródeł (atrybucją) cyberataków – co w konsekwencji przekłada się na niemożność wykorzystania przez państwa strategii odstraszania przez odwet. Po trzecie, cechy cyberprzestrzeni (takie jak np. możliwość zachowania do pewnego stopnia anonimowości) faworyzują stronę atakującą. Biorąc pod uwagę wymienione złożoności, można śmiało stwierdzić, że cyberdyplomacja stanowi obecnie kluczową dziedzinę stosunków międzynarodowych[10]. Do jej najważniejszych celów, uznanych np. przez UE, należy stworzenie otwartej, globalnej, bezpiecznej oraz stabilnej cyberprzestrzeni opartej na ustalonych pomiędzy krajami sojuszniczymi (a także organizacjami, sektorem prywatnym, podmiotami społeczeństwa obywatelskiego oraz ekspertami) normach i zasadach[11].

Obszarami, na których skupia się cyberdyplomacja, są m.in. międzynarodowe normy odpowiedzialnego zachowania w cyberprzestrzeni (ang. *norms of responsible behaviour in cyberspace*), środki budowy zaufania (ang. *confidence-building measures*) oraz zdolności w zakresie cyberbezpieczeństwa (ang. *cyber capacity*), a także stosowanie prawa międzynarodowego do cyberprzestrzeni. Obszarom tym przyjrzymy się w kolejnej części rozdziału, opisującej konkretne inicjatywy związane z budowaniem cyfrowego pokoju.

W STRONĘ CYFROWEGO POKOJU – INICJATYWY REGIONALNE I GLOBALNE

Współcześnie istnieje wiele inicjatyw oraz sojuszy mających na celu łagodzenie i rozwiązywanie konfliktów dotyczących cyberprzestrzeni. Różnią się one jednak formą, zasięgiem, profilem interesariuszy, a także celami. Cele te niekiedy pozostają rozbieżne, a osiągnięcie konsensusu na skalę globalną wydaje się aktualnie niemożliwe.

Jedne z najważniejszych procesów dotyczących ustalania światowych norm i zasad obowiązujących w cyberprzestrzeni odbywają się w obrębie Organizacji Narodów Zjednoczonych (ONZ). Centralny punkt dyskusji stanowi stosowalność istniejącego prawa międzynarodowego w cyberprzestrzeni. Obecnie kwestią sporną jest raczej pytanie nie „czy" ale „jak" prawo to powinno być interpretowane[12]. Obrady pierwszej powołanej w ramach ONZ grupy ekspertów rządowych (tzw. UN GGE) trwały w latach 2004–2005, jednak zakończyły się brakiem konsensusu wynikającym z rozbieżności co do ingerencji w krajowe systemy bezpieczeństwa informacji. Druga UN GGE, zainicjowana po serii cyberataków o charakterze politycznym (na Estonię oraz Gruzję w 2007 r. oraz na Litwę w 2008 r. – wszystkie atrybuowane Rosji[13]) obradowała w latach 2009–2010, a efektem jej pracy był raport podkreślający znaczenie dialogu pomiędzy państwami, budowy wzajemnego zaufania, wymiany informacji na temat krajowych strategii oraz potrzebę wspierania krajów słabiej rozwiniętych. Dalej idące oraz bardziej konkretne wnioski przedstawiła dopiero trzecia UN GGE działająca w latach 2012–2013. W konkluzjach grupy podkreślono, że prawo międzynarodowe, a w szczególności Karta ONZ, ma zastosowanie w cyberprzestrzeni oraz jest niezbędne do utrzymania pokoju, stabilności, a także promowania „otwartego, bezpiecznego, pokojowego i dostępnego środowiska ICT"[14]. W raporcie stwierdzono również, że państwa muszą wywiązywać się z międzynarodowych zobowiązań dotyczących działań niezgodnych z prawem. Czwarta UN GGE (2014–2015) w konkluzjach podkreśliła znaczenie zaangażowania sektora nauki i biznesu, zaleciła współpracę pomiędzy krajami w celu zapobiegania szkodliwym praktykom w cyberprzestrzeni oraz stwierdziła, że państwa nie powinny zezwalać na niezgodne z prawem działania dokonywane z ich terytorium.

a Mowa tutaj o Konwencji wiedeńskiej o stosunkach dyplomatycznych z 1961 roku, Konwencji wiedeńskiej o stosunkach konsularnych z 1963 r., Konwencji o misjach specjalnych z 1969 r. oraz o Konwencji wiedeńskiej dotyczącej reprezentacji państw w ich stosunkach z organizacjami międzynarodowymi o charakterze uniwersalnym z 1975 r.

b Angielski polityk i arystokrata, trzykrotny minister spraw zagranicznych i dwukrotny premier Wielkiej Brytanii.

c Estonia posiada nie tylko specjalnie powołanego Ambasadora, ale też cały Departament Cyberdyplomacji, funkcjonujący w ramach Ministerstwa Spraw Zagranicznych.

GEOPOLITYKA
NOWYCH TECHNOLOGII CYFROWYCH

Zidentyfikowała również szereg środków budowy zaufania. Obradująca w latach 2016–2017 piąta UN GGE zakończyła prace brakiem konsensusu, głównie z uwagi na rozbieżności w interpretacji zapisów prawa międzynarodowego dotyczących samoobrony oraz użycia siły proporcjonalnie do poniesionej szkody. Pod koniec 2018 r. na mocy uchwalonych rezolucji powstały dwie platformy mające doprecyzować zagadnienia interpretacji prawa międzynarodowego – kolejna, szósta grupa ekspertów rządowych oraz otwarta grupa robocza (UN OEWG[d]). Ogłoszenie wyników prac obu grup odbędzie się na Zgromadzeniach Ogólnych ONZ – odpowiednio w 2020 r. dla UN OEWG oraz w 2021 r. dla UN GGE[15].

Stosowanie prawa międzynarodowego w cyberprzestrzeni porusza również Tallinn Manual, inicjatywa o charakterze akademickim poświęcona praktycznym aspektom tego problemu. Dotychczas odbyły się dwie edycje – pierwsza w 2013 r. oraz druga, Tallinn Manual 2.0, w 2017 r. (pierwsza wersja odnosiła się do ataków i wojny w cyberprzestrzeni, druga natomiast została rozszerzona o incydenty nieprzekraczające progu konfliktu zbrojnego). Inicjatorem projektu było Centrum Eksperckie Sojuszu Północnoatlantyckiego – NATO CCD COE – mające siedzibę w Estonii[16].

W kontekście rozwoju cyberdyplomacji z punktu widzenia regionalnego na uwagę zasługują działania Unii Europejskiej, która w 2017 r. przyjęła tzw. *EU diplomacy toolbox*, wyznaczający ramy wspólnej unijnej reakcji dyplomatycznej na wrogie działania w cyberprzestrzeni[17]. Wytyczne dotyczą: środków zapobiegawczych (budowanie zaufania, zdolności oraz zwiększanie świadomości co do polityk UE), środków współpracy (dialogi polityczne), środków stabilności (oficjalne oświadczenia, konkluzje Rady UE, zaangażowanie dyplomatyczne na arenie międzynarodowej), środków ograniczających (sankcji– wśród nich zakazy podróży, embarga, zamrażanie aktywów nałożonych na rządy, organizacje czy osoby fizyczne) oraz wsparcia UE dla zgodnych z prawem reakcji państw członkowskich na kierowane przeciwko nim wrogie działania w cyberprzestrzeni[18]. Dokument odnosi się także do konieczności budowania wspólnej świadomości sytuacyjnej, możliwej dzięki wymianie informacji. Mimo że państwa członkowskie mogą podejmować suwerenne decyzje co do atrybucji szkodliwych działań w cyberprzestrzeni, niezbędna jest jednak szersza i zbiorowa ocena, aby wspólna odpowiedź UE była efektywna. W kwietniu 2018 r. Rada przyjęła kolejne konkluzje[19], potępiając destabilizujące cyberprzestrzeń incydenty takie jak WannaCry i NotPetya. Podkreśliła również znaczenie środków ograniczających (sankcji) mogących efektywnie przyczynić się do zapobiegania wrogim działaniom w cyberprzestrzeni. W nowo przyjętej strategii Komisji Europejskiej z lutego 2020 r. dotyczącej kształtowania cyfrowej przyszłości Europy[20] UE deklaruje również dalszą ścisłą współpracę z partnerami międzynarodowymi, m.in. z Grupą G7 w celu opracowania wspólnych międzynarodowych norm i standardów. W 2021 r. powstanie również tzw. Globalna Strategia Współpracy Cyfrowej, promująca europejski model transformacji cyfrowej.

W ramach współpracy Grupy G7 w kwietniu 2019 r. przyjęta została deklaracja o zapobieganiu szkodliwym działaniom w cyberprzestrzeni (tzw *Dinard Declaration on the Cyber Norm Initiative*)[21]. Światowe mocarstwa wyraziły gotowość do utworzenia Cyber Norm Initiative, która miałaby być poświęcona dzieleniu się dobrymi praktykami i doświadczeniami związanymi z zastosowaniem norm odpowiedzialnego zachowania w cyberprzestrzeni. Inicjatywa ta, jak wskazuje G7, mogłaby być komplementarna do obecnie trwających prac UN GGE oraz UN OEWG[22]. Odzwierciedlałaby także trend zacieśniania współpracy krajów podobnie myślących (ang. *like-minded*) w zakresie budowania bezpiecznego i demokratycznego świata cyfrowego.

d O ile skład UN GGE jest za każdym razem określany (od 15 do 25 ekspertów) z uwzględnieniem proporcji geograficznych oraz interesów krajowych (zawsze obejmując członków stałych Rady Bezpieczeństwa), o tyle w OEWG mogą wziąć udział wszystkie zainteresowane kraje będące członkami ONZ. W jej ramach prowadzone są również konsultacje z organizacjami pozarządowymi, niezależnymi ekspertami, a także sektorem prywatnym.

Sojuszem aktywnym w obszarze cyberdyplomacji, a w szczególności w rozwijaniu środków budowy zaufania, jest Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE). W 2016 r. rozszerzyła ona zapoczątkowaną w 2013 r. listę środków budowy zaufania mających na celu zmniejszenie ryzyka konfliktów, a także ich eskalacji, wynikających z wykorzystania technologii ICT. Dokument opisuje szesnaście środków (w 2016 r. dodano pięć) opierających się na zasadzie dobrowolności, dotyczących działań podejmowanych przez państwa. Należą do nich m.in.: prowadzenie konsultacji na odpowiednim poziomie w celu zmniejszenia ryzyka pojawienia się napięć lub konfliktów wynikających z korzystania z ICT, dzielenie się informacjami na temat środków podjętych w celu zapewnienia bezpieczeństwa sieci, promowanie partnerstw publiczno-prywatnych i opracowywanie mechanizmów wymiany dobrych praktyk dotyczących reagowania na wyzwania wynikające z zastosowania technologii ICT[23].

ROSNĄCE ZNACZENIE SEKTORA PRYWATNEGO W STOSUNKACH MIĘDZYNARODOWYCH

Udział sektora prywatnego, a przede wszystkim korporacji, w dialogu międzynarodowym jest znany historii od stuleci. Już w XVII wieku Kompania Wschodnioindyjska otrzymała szerokie uprawnienia do zawierania sojuszy politycznych, posiadania swojego wojska oraz wypowiadania wojny, co doprowadziło do podbicia przez nią niemal całego subkontynentu indyjskiego[24]. Współczesny proces globalizacji, a także zwiększająca się złożoność powiązań handlowych oraz prywatno-publicznych w gospodarce sprawiają, że w dialog polityczny włącza się coraz większa ilość podmiotów pozapaństwowych. Relacje międzynarodowe wpływają również na mniejsze przedsiębiorstwa, które są uzależnione od globalnych łańcuchów dostaw. Sektor prywatny narażony jest na wszelkie niebezpieczeństwa płynące z sieci, takie jak cyberszpiegostwo, cyberataki czy dezinformacja. Zagrożenia te często wynikają z działalności rządów, chcących dostać się do tajemnic gospodarczych państwa, wyrządzić szkody w postaci ataków paraliżujących gospodarkę, prowadzących do znaczących strat PKB, czy też w końcu podważyć reputację firmy działaniami dezinformacyjnymi. Udział podmiotów pozapaństwowych jest obecnie aktywnie wspierany przez politycznych decydentów. Konkluzje Rady UE dotyczące multilateralizmu[25] podkreślają, że „[z] najważniejszymi globalnymi wyzwaniami naszej ery możemy zmierzyć się wyłącznie poprzez pracę w partnerstwie z innymi: czy to państwami, czy organizacjami międzynarodowymi i regionalnymi, organizacjami społeczeństwa obywatelskiego, sektorem prywatnym, partnerami społecznymi i innymi podmiotami oraz poprzez wspieranie reform systemu wielostronnego".

Przykładem takich wielostronnych inicjatyw budowy pokoju w cyberprzestrzeni jest apel francuskiego rządu o nazwie Paris Call for Trust and Security in Cyberspace, a także działania Globalnej Komisji ds. Stabilności w Cyberprzestrzeni (ang. Global Commission on Stabilit in Cyberspace). Paris Call, zainicjowany w listopadzie 2018 r., zyskał do tej pory poparcie 78 krajów, 30 instytucji publicznych i samorządów lokalnych, prawie 350 organizacji i członków społeczeństwa obywatelskiego[e] oraz niemal 650 firm[26]. Pomimo bardzo szerokiego wsparcia wielkie światowe mocarstwa takie jak Stany Zjednoczone[f], Chiny czy Rosja oficjalnie nie poparły tego apelu. Celem tej inicjatywy, opierającej się na założeniu, że odpowiedzialność za cyberprzestrzeń leży w rękach wielu różnych podmiotów, jest wzmocnienie zaufania, bezpieczeństwa oraz stabilności cyfrowego świata. Paris Call wspiera także założenie o stosowaniu prawa międzynarodowego (w tym Karty Narodów Zjednoczonych, prawa humanitarnego, praw człowieka oraz międzynarodowego prawa zwyczajowego) w korzystaniu przez państwa z technologii ICT. W sumie Paris Call obejmuje

e Instytut Kościuszki był w pierwszej grupie organizacji, które poparły Paris Call w 2018 r.

f Apel wsparły jednak władze regionalne z USA – miasta Louisville w Kentucky i Huntington w Wirginii Zachodniej oraz stan Wirginia, a także wiele Amerykańskich Izb Handlowych z różnych części świata.

dziewięć zasad[27], wśród których znajdują się m.in.: ochrona integralności Internetu, współpraca w celu ochrony procesów wyborczych, ochrona własności intelektualnej oraz promocja powszechnego wdrażania norm odpowiedzialnego zachowania oraz środków budowy zaufania w cyberprzestrzeni.

Podmiotem zaangażowanym w proces budowania norm jest także wspomniana Globalna Komisja ds. Stabilności w Cyberprzestrzeni, powołana przez dwa niezależne think tanki – The Hague Centre for Strategic Studies oraz EastWest Institute. Komisja składa się z 26 Komisarzy[28] (wybitnej klasy ekspertów z całego świata), a jej prace wspierają fundatorzy reprezentujący sektor publiczny, prywatny oraz społeczeństwo obywatelskie[29]. Komisja proponuje swój zestaw norm, opracowanych w listopadzie 2019 r., adresując go zarówno do podmiotów państwowych, jak i niepaństwowych[30]. Wiele wątków zawartych w Paris Call oraz w owych normach dotyczy podobnych wyzwań takich jak ochrona systemów wyborczych i integralności Internetu czy cyberhigiena. Warto zaznaczyć, że Komisja znalazła się również na oficjalnej liście instytucji wspierających Paris Call.

PODSUMOWANIE – ZNACZENIE CYBERDYPLOMACJI W REGIONIE TRÓJMORZA

Złożoność cyberprzestrzeni i wynikające z niej wyzwania dla stosunków międzynarodowych sprawiają, że dyplomacja staje się niezbędnym środkiem w dążeniu do zapewnienia pokoju w cyfrowym świecie. Biorąc pod uwagę powyższe rozważania dotyczące rosnącego znaczenia tego obszaru, należy stwierdzić, że państwa regionu powinny szeroko wykorzystywać narzędzia cyberdyplomacji jako element wsparcia cyfrowej polityki gospodarczej i budowania pozycji w globalnym dialogu na temat przemian cyfrowych współczesnego świata. Decydenci w tej części Europy muszą nauczyć się nowej odpowiedzialności, jaką jest odpowiedzialność za cyberprzestrzeń. Wszystkie kraje regionu Trójmorza powinny m.in. powołać specjalne stanowisko koordynatora / ambasadora właściwego ds. cyberdyplomacji wspieranego przez departament ds. cyberdyplomacji[g] oraz aktywnie włączać się w dialog dotyczący stanowienia norm odpowiedzialnego zachowania w cyberprzestrzeni oraz środków budowy zaufania. Jako platforma dialogu oraz współpracy reprezentantów wszystkich krajów w kwestii cyberdyplomacji może posłużyć forum Inicjatywy Trójmorza. Nie bez znaczenia pozostaje umiejscowienie regionu, znajdującego się na zewnętrznej granicy UE, a także na wschodniej flance NATO, które kreuje charakterystyczne dla niego wyzwania, również związane z cyberprzestrzenią. Jak pokazała historia, kraje te bardzo często stanowią poligon doświadczalny dla wrogich operacji hybrydowych sponsorowanych przez państwa. Dlatego też wspólny głos dotyczący atrybucji owych operacji oraz zgodne reakcje na cyberataki mogą stanowić efektywne kroki w celu ograniczenia wrogich działań w cyberprzestrzeni.

g Warto rozważyć również powołanie tzw. tech ambasadorów.

PRZYPISY

1 Frelek R., *Dzieje dyplomacji, Zarys historii stosunków międzynarodowych*, Wydawnictwo Adam Marszałek, Toruń, 2006.

2 Molendowski E., Polan W., *Dyplomacja gospodarcza, rola i znaczenie w polityce zagranicznej państwa*, Oficyna, Kraków, 2007.

3 Bollier D., *The Rise of Netpolitik, How the Internet is changing the international politics and diplomacy*, The Aspen Institute, Washington DC, 2003.

4 Surmacz B., *Wpływ nowych technologii na funkcje współczesnej dyplomacji*, [w:] red. nauk. M. Kosienkowski, B. Piskorska, *Dyplomacja cyfrowa jako instrument polityki zagranicznej XXI wieku*, Katolicki Uniwersytet Lubelski Jana Pawła II. Wydział Nauk Społecznych. Katedra Stosunków Międzynarodowych, Lublin, 2004.

5 Cyber Peace Alliance, *Cyber Diplomacy: Governance Beyond Government*, Medium, 12.10.2019, [online:] https://medium.com/@cyberpeacealliance/cyber-diplomacy-governance-beyond-government-e8b92effff8f.

6 *Cyber diplomacy in the European Union*, EU Cyber Direct, 12.2019, [online:] https://eucyberdirect.eu/wp-content/uploads/2019/12/cd_booklet-final.pdf.

7 Latici T., *Understanding the EU's approach to cyber diplomacy and cyber defence*, European Parliamentary Research Service Briefing, 2020.

8 CyberPeace Alliance, *Cyber Diplomacy: Governance Beyond Government*, Medium, 12.10.2019, [online:] https://medium.com/@cyberpeacealliance/cyber-diplomacy-governance-beyond-government-e8b92effff8f.

9 Latici T., *Understanding the EU's approach to cyber diplomacy and cyber defence*, European Parliamentary Research Service Briefing, 2020.

10 Barrinha A., Renard T., *Cyber-diplomacy: the making of an international society in the digital age*, Global Affairs, 2017.

11 Latici T., *Understanding the EU's approach to cyber diplomacy and cyber defence*, European Parliamentary Research Service Briefing, 2020.

12 Delerue F., Kulesza J., Pawlak P., *The Application of International Law in Cyberspace: Is There a European Way?*, EU Cyber Direct, 04.2019 [online:] https://eucyberdirect.eu/wp-content/uploads/2019/05/delerue_kulesza_pawlak-international-law-in-cyberspace-european-way-april-2019-eucyberdirect_.pdf.

13 Balcewicz J., *UN GGE – prawo międzynarodowe w cyberprzestrzeni*, NASK Cyberpolicy, 15.01.2020, [online:] https://cyberpolicy.nask.pl/un-gge-prawo-miedzynarodowe-w-cyberprzestrzeni/#_ftn1.

14 Tamże.

15 Tamże.

16 *Tallinn Manual 2.0*, CCDCOE, 2017, [online:] https://ccdcoe.org/research/tallinn-manual/.

17 *Cyber-attacks: Council is now able to impose sanctions*, European Council Press Release, 17.05.2019, [online:] https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

18 *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text*, Council of the European Union, 13007/17, 09.10.2017, [online:] https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

19 *Konkluzje Rady w sprawie szkodliwych działań w cyberprzestrzeni – zatwierdzenie*, Rada Unii Europejskiej, 7925/18, 16.04.2018, [online:] http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/pl/pdf.

20 *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions. Shaping Europe's digital future*, European Commission, 19.02.2020, [online: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf.

21 *G7 foreign ministers adopt the 'Dinard Declaration on the Cyber Norm Initiative'*, GIP Digital Watch, 06.04.2019, [online:] https://dig.watch/updates/g7-foreign-ministers-adopt-dinard-declaration-cyber-norm-initiative.

22 *Dinard Declaration on Cyber Norm Initiative*, G7 Information Centre, 06.04.2019, [online:] http://www.g7.utoronto.ca/foreign/190406-cyber.html.

23 *Decision No. 1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies*, Organization for Security and Co-operation in Europe, 10.06.2016, [online:] https://www.osce.org/files/f/documents/d/a/227281.pdf.

24 Blakemore E., *How the East India Company became the world's most powerful business*, 06.09.2019, [online:] https://www.nationalgeographic.com/culture/topics/reference/british-east-india-trading-company-most-powerful-business/.

25 *Działanie UE na rzecz wzmocnienia multilateralizmu opartego na zasadach – Konkluzje Rady (17 czerwca 2019)*, Rada Unii Europejskiej, 10341/19, 17.06. 2019, s. 3, [online:] https://data.consilium.europa.eu/doc/document/ST-10341-2019-INIT/pl/pdf.

26 *Paris Call*, Paris Call for Trust and Security in Cyberspace, 11.12.2018, [online:] https://pariscall.international/en/.

27 *The 9 Principles*, Paris Call for Trust and Security in Cyberspace, 11.12.2018, [online:] https://pariscall.international/en/principles.

28 *Commissioners*, The Global Commission on the Stability of Cyberspace, 2020, [online:] https://cyberstability.org/commissioner/.

29 Global Commission on the Stability of Cyberspace, 2020, [online:] https://cyberstability.org/about/.

30 Normy znajdują się na s. 21 raportu *Advancing Cyberstability, Final Report, November 2019*, Global Commission on the Stability of Cyberspace, 09.2019, [online:] https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf.

Robert Siudak

NOWE PODMIOTY W MULTILATERALNYM CYBERŚWIECIE

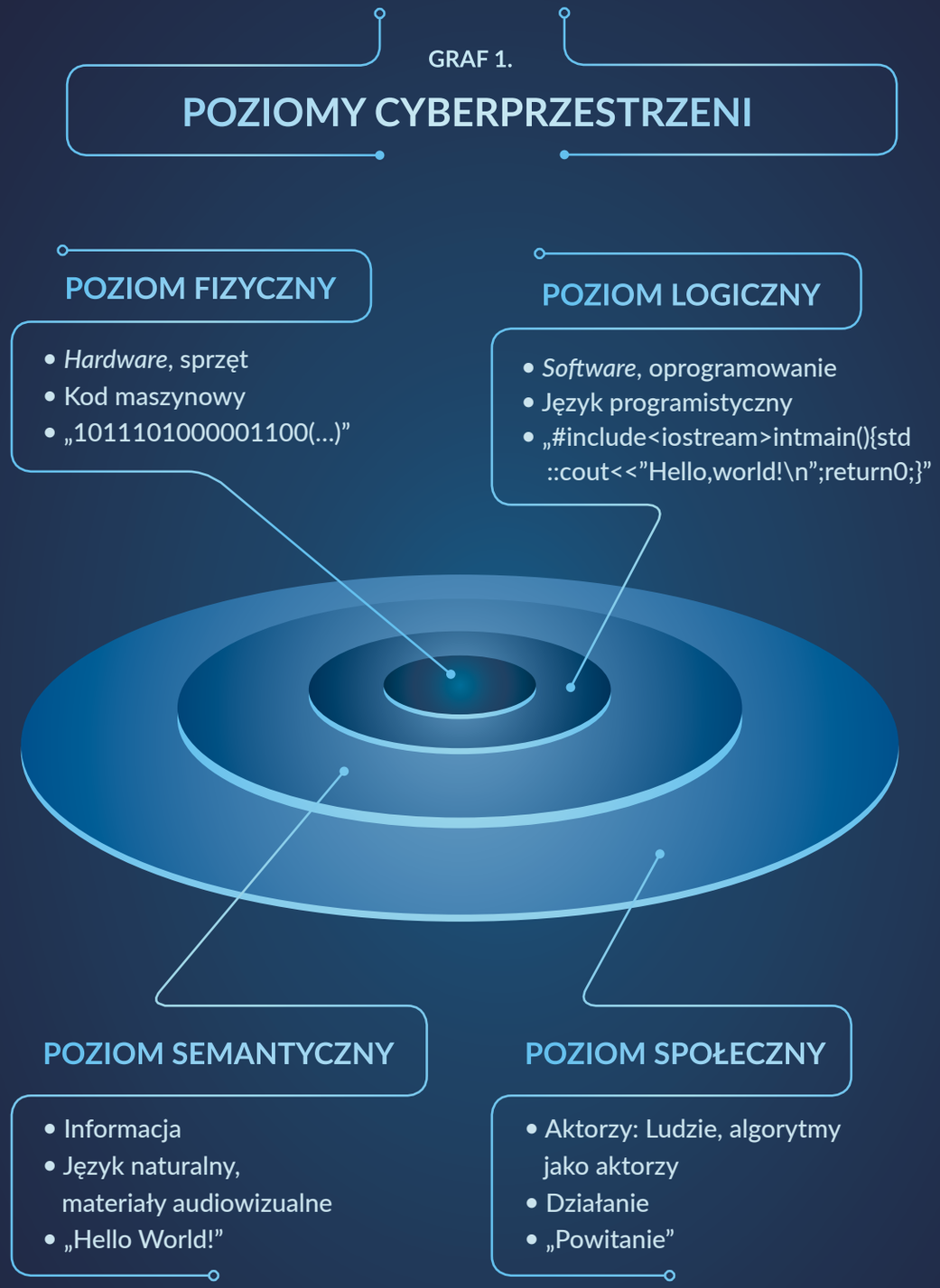
Zarówno historia, struktura, jak i określone cechy cyberprzestrzeni jako domeny działań jednostek, organizacji oraz krajów decydują o kluczowej roli podmiotów pozapaństwowych w debacie na temat teraźniejszości oraz przyszłości cyfrowego świata. Szczególną pozycję w jego multilateralnej strukturze zajmują firmy technologiczne, które historycznie w wielu wypadkach odgrywać musiały w cyberprzestrzeni równocześnie rolę twórcy, regulatora, uczestnika i sędziego. Sytuacja ta dynamicznie zmienia się wraz z coraz większym zaangażowaniem zarówno państwa, jak i organizacji międzynarodowych w kształtowanie ram funkcjonowania cyberprzestrzeni, szczególnie w kontekście bezpieczeństwa tej domeny. Mechanizmy współpracy pomiędzy klasycznymi podmiotami relacji międzynarodowych w ujęci systemu westfalskiego, takimi jak państwa czy sojusze, a nowymi graczami w cyberświecie, takimi jak korporacje międzynarodowe czy ponadnarodowe grupy eksperckie (tzw. wspólnoty epistemiczne), wykuwają się na naszych oczach.

TECHNOLOGIA JAKO NARZĘDZIE KSZTAŁTOWANIA CYBERŚWIATA

Według stanu na marzec 2020 r., siedem pierwszych miejsc na liście najwyżej wycenianych rynkowo firm na świecie (według kapitalizacji giełdowej) stanowią korporacje technologiczne. Zgodnie z kolejnością są to: Microsoft, Apple, Amazon, Alphabet, Alibaba Group, Facebook oraz Tencent[1]. Jednak to nie same zasoby kapitału stanowią o sile i pozycji gigantów technologicznych w zakresie określania reguł cyberprzestrzeni. Oczywiście dostęp do najwyższej klasy pracowników IT, rozbudowanej infrastruktury oraz zasobów danych, o jakich większość państw nie może nawet

GRAF 1.

POZIOMY CYBERPRZESTRZENI



Opracowanie własne na podstawie: Libicki, M., *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York, 2007; Clark, D., *Characterizing Cyberspace: Past, Present, and Future*, ECIR Working Paper 2010, [online:] https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf.

marzyć, ma znaczenie. Jednak **centralna rola firm technologicznych w kreacji oraz zabezpieczaniu cyfrowego świata wynika z podstawowego faktu: to one tworzą, utrzymują oraz dystrybuują globalnie i lokalnie technologie, które leżą u podstaw funkcjonowania współczesnej cyberprzestrzeni.**

Aby zrozumieć ich pozycje w tym kontekście, warto odnieść się do samej struktury cyfrowego świata. Często wskazuje się w tym wypadku na cztery poziomy cyberprzestrzeni: (1) fizyczny, (2) logiczny, (3) semantyczny oraz (4) społeczny. Szerzej opisano je na grafie X. Patrząc z perspektywy roli pozapaństwowych aktorów, należy zwrócić uwagę na kluczowe znaczenie firm technologicznych na dwóch pierwszych poziomach, ale także aktywną postawę w zakresie regulacji pozostałych dwóch wymiarów. Z kolei historię zaangażowania państw narodowych w kształtowanie cyberprzestrzeni w uproszczeniu przedstawić można jako stopniowe i powolne rozszerzanie roli regulatora oraz aktora od poziomu czwartego aż do pierwszego[a].

To właśnie poziom sprzętu oraz oprogramowania bezpośrednio wyznacza zasady funkcjonowania cyberprzestrzeni. Słynna fraza „Code is Law” (kod jest prawem)[2] ukuta jeszcze pod koniec XX wieku dotyczy właśnie tej kluczowej roli oprogramowania w kształtowaniu ram cyfrowego świata. Jeszcze bardziej aktualnego znaczenia nabierają te słowa w kontekście rozwoju sztucznej inteligencji oraz systemów autonomicznych i implikacji etycznych oraz społecznych z tym związanych. Globalne korporacje technologiczne posiadają w tym punkcie kluczową siłę kreacyjną, ale tym samym wielkie zobowiązanie względem miliardów użytkowników z różnych części świata, z odmiennych, krajów, kultur czy społeczeństw. W ramach projektowania oraz implementowania określonych narzędzi technologicznych są w stanie wpływać znacząco na poziom bezpieczeństwa globalnej gospodarki cyfrowej. Przykładem mogą być aktualne działania firm takich jak Alphabet, Microsoft czy Apple dotyczące zmian polityk bezpieczeństwa ich przeglądarek internetowych. Decyzją producentów, przeglądarki te jako „niezaufane” oznaczają domeny korzystające ze starych, mniej bezpiecznych wersji protokołów chroniących komunikację internetową – SSL/TLS. W ramach aktualizacji przewidzianych na rok 2020 zarówno Chrome, Edge, jak i Safari przestaną rozpoznawać jako bezpieczne połączenia z wykorzystaniem przestarzałych wersji TLS 1.0 oraz TLS 1.1. Tylko z pierwszej z przytoczonych przeglądarek korzysta szacunkowo ponad 3 miliardy użytkowników na całym świecie[3]. Oznacza to bezpośredni wpływ na bezpieczeństwo funkcjonowania w cyberprzestrzeni większej ilości obywateli, niż ma pod swoją jurysdykcją jakikolwiek kraj na świecie.

MULTILATERALIZM JAKO ODPOWIEDŹ NA PROBLEMY CYFROWEJ POLITYKI MIĘDZYNARODOWEJ

Bezpośrednie narzędzia techniczne to nie jedyny wymiar zaangażowania podmiotów pozapaństwowych w tworzenie reguł cyberświata. Kolejnym poziomem są działania na rzecz ustanawiania globalnych norm, dobrych praktyk, a także praw zachowania w cyberprzestrzeni. Trwające do tej pory na forum Organizacji Narodów Zjednoczonych (ONZ) oraz Międzynarodowego Związku Telekomunikacyjnego (ang. International Telecommunication Union, ITU) próby zmierzające do ustanowienia szerokiego międzynarodowego porozumienia dotyczącego bezpieczeństwa cyberprzestrzeni, którego sygnatariuszami byłyby państwa narodowe, należy uznać za fiasko. Jednak równolegle do nich szereg podmiotów zarówno publicznych, jak i prywatnych podejmuje działania mające na celu stworzenie otwartych międzynarodowych form współpracy i dyskusji nad kształtem oraz bezpieczeństwem cyberprzestrzeni. W przeciwieństwie do postulatów

a Podsumowanie to nie dotyczy okresu wykluwania się samych technologii sieciowych (ARPANET oraz jego następstwa) czy wąsko rozumianych technologii podwójnego zastosowania (np. kryptograficznych), co do regulacji których państwa narodowe od początku rościły sobie i roszczą daleko idące prerogatywy. Mowa w tym wypadku o szeroko rozumianej cyberprzestrzeni, w której uczestniczą masowo obywatele, a która także stanowi podstawę cyfrowych gospodarek.

promowanych na forum ONZ przez takie państwa jak Rosja czy Chiny, uwzględniają one kluczową rolę nie tylko administracji rządowych, ale także sektora prywatnego, akademii oraz wyspecjalizowanych podmiotów funkcjonujących w ramach społeczeństwa obywatelskiego.

Jednym z najbardziej rozpoznawalnych przykładów jest działające od 2006 pod auspicjami ONZ Forum Zarządzania Internetem (ang. Internet Governance Forum, IGF). Zostało ono powołane na podstawie decyzji podjętej podczas Światowego Szczytu Społeczeństwa Informacyjnego (ang. The World Summit on the Information Society, WSIS) z roku 2005. W gronie donatorów i aktywnych uczestników IGF znajdują się m.in. Komisja Europejska, ICANN, USA, Holandia, Wielka Brytania, ale też Microsoft, Google, AT&T czy Facebook. IGF w roku 2016 powołało do życia forum dobrych praktyk w zakresie cyberbezpieczeństwa, a już rok później opublikowano pierwsze konkluzje jego prac. Wskazano przede wszystkim na rolę bezpieczeństwa cyfrowego jako niezbędnego elementu rozwoju ICT umożliwiającego osiągnięcie Celów Zrównoważonego Rozwoju ONZ (ang. Sustainable Development Goals, SDGs)[4]. Najbardziej rozpoznawalnym elementem prac IGF pozostają coroczne szczyty, podczas których podejmowane są decyzje kierunkowe dotyczące prac Forum. W roku 2018 odbył się on w Paryżu, w 2019 w Berlinie. Podczas szczytu odbywającego się we Francji prezydent Emmanuel Macron przedłożył deklarację „Paryskie wezwanie do zaufania i bezpieczeństwa w cyberprzestrzeni" (ang. Paris Call for Trust and Security in Cyberspace), zapraszając wszystkie zainteresowane strony, nie tylko państwa, do podpisania odezwy. Według stanu na 27 czerwca 2020 r. pod wezwaniem oprócz szeregu państw i organizacji trzeciego sektora, podpisało się 646 firm. Z samej Polski 25 pozapaństwowych podmiotów jest sygnatariuszem porozumienia, w tym firmy technologiczne, think tanki, izby branżowe oraz organizacje otoczenia biznesu[b].

W kontekście promocji międzynarodowych norm działania w cyberprzestrzeni przez podmioty pozapaństwowe warto także pokrótce odnieść się do inicjatyw branży technologicznej. Firma Microsoft w roku 2017, ustami swojego prezesa Brada Smitha, wezwała państwa do stworzenia i podpisania Cyfrowej Konwencji Genewskiej (ang. Digital Geneva Convention)[5]. Oryginalne konwencje genewskie to zestaw czterech traktatów podpisanych w roku 1949 regulujących działania wojenne w kontekście ochrony cywilów oraz jednostek wykluczonych z walki. Założeniem Konwencji Genewskiej 5.0 proponowanej przez Microsoft jest prawne uregulowanie działań państw w cyberprzestrzeni w celu ochrony postronnych użytkowników[6]. Kolejnym krokiem było podpisanie w roku 2018 porozumienia Cybersecurity Tech Accord, którego sygnatariuszami obok firmy z Redmond jest ponad 100 przedsiębiorstw technologicznych głównie z USA oraz UE, w tym m.in. ABB, Oracle, RSA, Cisco, Dell, Nokia czy SAP[8]. W październiku tego samego roku, podczas Europejskiego Forum Cyberbezpieczeństwa CYBERSEC 2018, do tego grona dołączyło pierwsze 7 firm z regionu Trójmorza, w tym z Polski. Cztery główne zasady zawarte w ramach porozumienia to:

- „Ochrona wszystkich użytkowników i klientów na całym świecie;
- Przeciwstawianie się cyberatakom na niewinnych obywateli i przedsiębiorstwa bez względu na ich lokalizację;
- Wspieranie użytkowników, klientów i programistów, aby wzmocnili swoją ochronę na rzecz cyberbezpieczeństwa;
- **Ścisła współpraca zarówno w ramach porozumienia, jak i z grupami o podobnym podejściu do kwestii cyberbezpieczeństwa"[9].**

b American Chamber of Commerce in Poland, Axence, Billennium, CEC Government Relations, Center for Propaganda and Disinformation Analysis, Centre for International Relations (CSM), Cyberus Labs, Digital Fingerprints, Digital Poland Foundation, Domański Zakrzewski Palinka, ePaństwo Foundation, Foundation for the Prevention of Cybercrime (FPC), Integrity Partners, Konfederacja Lewiatan, NGL Wiater sp.k. (NGL Legal), Polish Hospital Federation, Polityka Insight, Predica, ProtectHut, Silesian Catalysts, SK&S Legal, The Kosciuszko Institute, The Polish Chamber of Information Technology and Telecommunications, THINKTANK – Centre for Dialogue and Analysis, ZIPSEE Digital Poland

Warto dodać, że w tym samym roku, w którym Microsoft ogłosił Tech Accord, na Monachijskiej Konferencji Bezpieczeństwa Siemens przedłożył porozumienie Charter of Trust, którego celem jest „ustanowienie wiążących zasad i standardów na rzecz zbudowania zaufania do cyberbezpieczeństwa i dalszego rozwoju cyfryzacji"[10]. Wśród jego 16 sygnatariuszy znalazły się głównie europejskie firmy takie jak Airbus, Allianz, Atos, Daimler, Deutsche Telekom, ale też IBM oraz Dell Technologies.

Ważne przykłady aktywnego włączania się w debatę dotyczą kształtu cyfrowego świata przez podmioty pozapaństwowe znaleźć można nie tylko na poziomie globalnym, ale także regionalnym. Przykładem jest inicjatywa AI Challengers, stworzona przez 19 izb branżowych, stowarzyszeń pracodawców oraz organizacji trzeciego sektora z Regionu Trójmorza[11]. Jej celem jest wypracowywanie rekomendacji oraz propozycji działań w zakresie planów rozwoju sztucznej inteligencji na Jednolitym Europejskim Cyfrowym Rynku. Współpraca różnorodnych interesariuszy w ramach jednej platformy wymiany wiedzy oraz opinii ma na celu tworzenie propozycji rozwiązań w zakresie polityk publicznych uwzględniających zarówno perspektywę biznesową, technologiczną, jak i społeczną, a także specyfikę potrzeb krajów i gospodarek Europy Środkowo-Wschodniej.

MIEJSCE KRAJÓW TRÓJMORZA W MULTILATERALNYM CYBERŚWIECIE

Wzrastająca rola cyberprzestrzeni stanowi z pewnością jeden z ważnych czynników transformacji systemu międzynarodowego w stronę ładu postwestfalskiego, opartego na współzależności oraz przenikaniu się prerogatyw krajów, organizacji międzynarodowych, ciał ponadnarodowych, a także globalnych korporacji i wspólnot epistemicznych. W tym kontekście należy zadać kluczowe pytanie o to, jaką strategię względem nowych aktorów ładu międzynarodowego, takich jak m.in. globalne firmy technologiczne, powinny przyjąć państwa. Oczywiście odpowiedź zależeć będzie od samej charakterystyki krajów i inaczej wyglądać będzie w wypadku mocarstw globalnych czy regionalnych, a inaczej w kontekście krajów średnich czy małych. W wypadku krajów regionu Trójmorza, w tym Polski, wskazać należy zarówno na potrzebę aplikacji tradycyjnego instrumentarium polityczno-ekonomicznego państw średnich, jak i budowy nowych narzędzi, nie obecnych w „standardowym" zestawie działań wykorzystywanych w ramach międzypaństwowych stosunków międzynarodowych.

Pierwszym z takich działań powinno być aktywne rozwijanie TechPlomacji (ang. *TechPlomacy*). Opiera się ona na budowie kanałów oraz inicjatyw dyplomatycznych państwa, zorientowanych z jednej strony na reprezentację interesów kraju w dialogu z globalnymi firmami technologicznymi, z drugiej na kształtowaniu szerszej multilateralnej debaty na temat ram i bezpieczeństwa cyfrowego świata[12]. Prekursorem w tym zakresie jeszcze w roku 2017 stała się Dania, która jako pierwszy kraj na świecie utworzyła osobny urząd *tech ambasadora*, o globalnym mandacie działania, a także biurach w Dolinie Krzemowej, Kopenhadze oraz Pekinie. Drugim narzędziem ze standardowego zestawu areny stosunków międzynarodowych, które znacznie zwiększa skuteczność działania krajów średnich w omawianym kontekście, jest tworzenie sojuszy celowych przez grupy państw. Przykładem jest sam Jednolity Rynek Cyfrowy w Unii Europejskiej (JRC). Dzięki zgromadzeniu ponad 500 milionów obywateli-konsumentów regulacje obejmujące ten rynek, takie jak np. Ogólne rozporządzenie o ochronie danych, wymuszają globalne zmiany w zakresie funkcjonowania usług cyfrowych. Warto także wskazać na przykład działania wewnątrz samego JRC, jakim była zapoczątkowana jeszcze w 2016 przez Polskę kampania dotycząca praktycznego umożliwienia swobodnego przepływu danych

nieosobowych. Czternaście krajów wsparło oficjalnie tę zakończoną sukcesem inicjatywę: Belgia, Bułgaria, Czechy, Dania, Estonia, Irlandia, Łotwa, Litwa, Luksemburg, Holandia, Słowenia, Szwecja i Wielka Brytania[13]. *Rozporządzenie o swobodnym przepływie danych nieosobowych w Unii Europejskiej* weszło w życie w 18 czerwca 2019 roku[14].

Nowy charakter cyberprzestrzeni często wymaga od władz państwowych wyjścia poza standardowe narzędzia realizacji polityk publicznych w celu odpowiedzi na poszczególne wyzwania związane m.in. z bezpieczeństwem cyfrowego świata. Przykładem takich działań może być tworzenie dedykowanych platform lub mechanizmów współpracy pomiędzy poszczególnymi organami państwa a firmami technologicznymi w określonym celu. W tym kontekście polski Program Współpracy w Cyberbezpieczeństwie (PWCyber) prowadzony przez Ministerstwo Cyfryzacji ma na celu:

1. „Podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni […].
2. Identyfikacja podatności i zagrożeń, wymiana informacji oraz wypracowywanie metod zgłaszania i obsługi incydentów, w tym również organizacja i udział w ćwiczeniach.
3. Opracowywanie rekomendacji w zakresie konfiguracji urządzeń, oprogramowania i usług w sposób maksymalizujący skuteczność mechanizmów zabezpieczających (ang. *Security Baselines*).
4. Przygotowanie i prowadzenie oceny oraz certyfikacji cyberbezpieczeństwa produktów i usług.
5. Promowanie innowacyjnych rozwiązań i projektów w dziedzinie cyberbezpieczeństwa oraz budowanie partnerstwa z podmiotami Krajowego Systemu Cyberbezpieczeństwa […]”[15].

Jego partnerami zostały do tej pory m.in. takie firmy technologiczne jak Ericsson, Cisco, Nokia, IBM, Samsung, Thales oraz Krypton. Innym przykładem nowych formatów działania może być współpraca instytucji publicznych lub spółek państwowych z międzynarodowymi firmami telekomunikacyjnymi w celu budowy bezpiecznej oraz szeroko dostępnej sieci 5G. Wypracowanie innowacyjnego modelu współpracy w tym zakresie ma na celu zapewnienie zarówno bezpieczeństwa infrastruktury dla klientów publicznych i służb porządkowych, jak i dostępności pasma oraz zysków komercyjnych dla operatorów telekomunikacyjnych. Próbę taką podejmuje projekt #Polskie5G, w ramach którego Polski Fundusz Rozwoju, Exatel oraz operatorzy aktywni w kraju (Orange, Polkomtel, T-Mobile oraz Play) próbują wypracować reguły współpracy umożliwiające wykorzystanie jednej infrastruktury oraz jednego pasma (700 MHz) w celu uruchomienia hurtowego ogólnopolskiego operatora sieci 5G[16].

PODSUMOWANIE

Rozwój cyberprzestrzeni stanowi sam w sobie wyzwanie dla tradycyjnie pojmowanych relacji międzynarodowych, między innymi ze względu na rolę, jaką odgrywają w niej pozapaństwowi aktorzy tacy jak firmy technologiczne czy sieci ponadnarodowych ekspertów. Jednocześnie zmieniająca się rola technologii cyfrowych stanowi szansę dla tych państw oraz organizacji międzynarodowych, które potrafią przemodelować swoje działania, dopasowując odpowiednio narzędzia oraz cele polityki zagranicznej, handlowej, rozwojowej, a nawet obronnej. Transformacja cyfrowa staje się zadaniem nie tylko dla firm czy gospodarek, ale także polityków oraz strategii narodowych.

PRZYPISY

1 *Largest Companies by Market Cap Today*, Dogs of the Dow, 10.06.2020, [online:] https://www.dogsofthedow.com/largest-companies-by-market-cap.htm.

2 Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, New York 1999.

3 Liczba użytkowników Internetu – 4,6 miliarda, za: Internet World Stats, *Internet Users Distribution in the World – 2020 Q1*, 10.06.2020, [online:] https://www.internetworldstats.com/stats.htm; udział Chrome to ok. 65%, za: StatsCounter, *Desktop Browser Market Share Worldwide*, 10.06.2020, [online:] https://gs.statcounter.com/browser-market-share/desktop/worldwide.

4 *IGF 2017*, *Best Practice Forum on Cybersecurity*, Internet Governance Forum, 01.2018, [online:] http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/1017.

5 Guay J., Rudnick L., *What the Digital Geneva Convention means for the future of humanitarian action*, The Policy Lab, UNHCR, 25.06.2017, [online:] https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.

6 *A Digital Geneva Convention to protect cyberspace*, Microsoft Policy Papers, 10.06.2020, [online:] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

7 Digital Peace Now Website, 10.06.2020, [online:] https://digitalpeace.microsoft.com.

8 *2018 In Review*, Cybersecurity Tech Accord, 10.06.2020, [online:] https://cybertechaccord.org/uploads/prod/2019/03/2018report.pdf.

9 Klimczuk A., *Rośnie globalna koalicja na rzecz cyfrowego bezpieczeństwa. Trzy polskie firmy w inicjatywie Cybersecurity Tech Accord*, 08.10.2018, [online:] https://news.microsoft.com/pl-pl/2018/10/08/rosnie-globalna-koalicja-na-rzecz-cyfrowego-bezpieczenstwa-trzy-polskie-firmy-w-inicjatywie-cybersecurity-tech-accord/.

10 *The Charter of Trust takes a major step forward to advance cybersecurity*, Siemens AG, 08.04.2020, [online:] https://www.siemens.com/press/en/feature/2018/corporate/2018-02-cybersecurity.php.

11 Panayotova A., *Central Europe wants to be heard in developing regulation on AI*, 13.02.2020, [online:] https://www.digitalalliance.bg/post/2020/02/13/central-europe-wants-to-be-heard-in-developing-regulation-on-ai.

12 *What is TechPlomacy*, Office of Denmark's Tech Ambassador, 10.06.2020, [online:] https://techamb.um.dk/en/techplomacy/abouttechplomacy/.

13 Widzyk A., *Polska na czele koalicji 14 krajów UE za swobodnym przepływem danych*, Forsal.pl, 02.12.2016, [online:] https://forsal.pl/artykuly/998321,polska-na-czele-koalicji-14-krajow-ue-za-swobodnym-przeplywem-danych.html.amp.

14 *Rozporządzenie (UE) 2018/1807 w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej z dnia 14 listopada 2018*, Parlament Europejski oraz Rada UE, PE/53/2018/REV/1.

15 Kośla R., *Program Współpracy w Cyberbezpieczeństwie (PWCyber)*, Ministerstwo Cyfryzacji, Departament Cyberbezpieczeństwa, Warszawa, 2019.

16 *Polskie 5G nabiera kształtów*, Ministerstwo Cyfryzacji, 28.10.2019, [online:] https://www.gov.pl/web/cyfryzacja/polskie-5g-nabiera-ksztaltow.

Izabela Albrycht

SIŁA CYFROWYCH DANYCH

Znaczenie danych generowanych dzięki technologiom cyfrowym i przesyłanych Internetem wykładniczo rośnie. W rezultacie świat jest w coraz większym stopniu napędzany danymi, które mają znaczenie nie tylko w wymiarze geoekonomicznym, ale również geopolitycznym. Już dziś widzimy, że rywalizacja strategiczna między mocarstwami toczy się także o dostęp i wykorzystanie danych, taką naturę ma bowiem cyfrowa zimna wojna rozgrywająca się między USA a ChRL. W przyszłości także konflikty międzynarodowe mogą przybrać postać walki o dane, a dzięki dostępowi do dużych zbiorów danych i ich odpowiedniej analizie budowane będą przewagi na polu walki. Dane w połączeniu z możliwościami sztucznej inteligencji są i – w znacznie większej skali niż obecnie – będą bowiem przekształcane w wysokiej jakości informacje, wiedzę oraz tzw. *insights*, znajdując jeszcze częstsze zastosowanie w sferze publicznej, działaniach informacyjnych, procesach decyzyjnych czy operacjach militarnych. Będą zatem generatorem różnego rodzaju wartości (ang. *value creation*). Dane są także fundamentem nowych i przełomowych technologii (ang. *emerging and disruptive technologies*), począwszy od wspomnianej już sztucznej inteligencji (ang. *artificial intelligence*), poprzez rozproszone rejestry (ang. *blockchain*), Internet Rzeczy (ang. *Internet of Things*), chmurę obliczeniową (ang. *cloud computing*) po analizę danych (ang. *Big Data and Advanced Analytics*). Tym samym decydować będą o strategicznej autonomii i suwerenności cyfrowej krajów oraz ich pozycji geotechnologicznej, wynikającej z możliwości kontroli procesu wytwarzania rozwiązań technologicznych i w konsekwencji zwiększenia możliwości projekcji siły i budowania przewag geopolitycznych i geoekonomicznych przez państwa[1]. Dlatego już dziś eksperci uznają, że dane oraz generowane dzięki nim informacje są najbardziej znaczącym i atrakcyjnym zasobem geopolitycznym[2].

Dane będą także generatorem jeszcze większego, niż ma to miejsce obecnie, zysku biznesowego poprzez stosowanie ich w modelach biznesowych (ang. *data-centric business models*) coraz większej ilości firm, a także prawdopodobnej dalszej konsolidacji pozycji rynkowej i międzynarodowego znaczenia platform cyfrowych, które stały się ważnymi aktorami w cyfrowym świecie.

Ponieważ zbieranie, przechowywanie, kontrola, analiza i odpowiednie wykorzystanie danych cyfrowych jest warunkiem *sine qua non* przyszłej potęgi gospodarczej, politycznej i militarnej krajów i regionów, to umiejętność ich wykorzystania już teraz dzieli świat na „front-runnerów", czyli USA oraz Chiny, i tych, którzy pozostają w tyle i jeszcze bardziej pogłębiają swoje zapóźnienie gospodarcze, czyli kraje rozwijające się i słabo rozwinięte. Stąd międzynarodowe instytucje takie jak Organizacja Narodów Zjednoczonych apelują o ustanowienie właściwych polityk, regulacji i narodowych strategii, aby cyfrowa gospodarka, której podstawą są dane i technologie ICT, a która stanowi integralną i nierozerwalną część gospodarki światowej, generowała wartość dla wielu, a nie jedynie dla kilku krajów[3]. ONZ wskazuje, że państwa z ograniczonymi możliwościami i umiejętnościami zamiany danych w wysokiej jakości informacje i szanse biznesowe są w niekorzystnym położeniu, jeśli chodzi o tworzenie wartości[4]. Obrazowo przedstawił ten proces na Forum Ekonomicznym w Davos Yuval Noah Harari, który stwierdził, że kraje posiadające wystarczająco dużo danych nie muszą wysyłać żołnierzy do kraju, aby go przejąć. Z kolei kraje, które nie nadążą w tym wyścigu, prawdopodobnie zbankrutują albo staną się koloniami danych (ang. *data colonies*)[5]. Z tych wszystkich względów obserwujemy w ostatnim czasie wzmożone działania mające na celu ochronę i kumulowanie danych cyfrowych przez państwa, organizacje i korporacje oraz często także odchodzenie od idei swobodnego przepływu danych pomiędzy granicami krajów. Chiny, Rosja, Iran czy Korea Północna starają

się od wielu lat zabezpieczyć granice „swojego Internetu" m.in. po to, aby chronić dane i informacje tworzone na platformach cyfrowych przez własnych obywateli i rezydentów. Podobnie, w najbliższym czasie wiele innych krajów może chcieć stworzyć swój „krajowy internet" albo połączyć się w grupy wokół wymienionych krajowych sieci internetowych. Stać się tak może nie tylko, aby kontrolować internet jako narzędzie komunikacyjne, ale także aby uzyskać i utrzymać kontrolę nad danymi w ramach narodowych granic bądź w ramach bloków geopolitycznych, połączonych wspólnymi celami geostrategicznymi.

GENEZA, TYPOLOGIA I WZROST ILOŚCI DANYCH

Dane cyfrowe to „szczegółowe, możliwe do maszynowego odczytu informacje dostępne praktycznie o wszystkim"[6]. Pierwszym sposobem ich generowania było nadawanie cyfrowego formatu danym i informacjom analogowym poprzez ich digitalizację[7]. Następnie trend ten przyspieszył, kiedy dane zaczęły być rezultatem aktywności coraz większej ilości użytkowników w Internecie, głównie na platformach cyfrowych. Konsekwencją korzystania przez nich z cyfrowych produktów i usług są pozostawiane cyfrowe ślady działalności prywatnej, towarzyskiej czy biznesowej[8]. Coraz bardziej zaawansowana jest także tzw. datafikacja (lub danetyzacja), polegająca na „narastającym procesie tworzenia cyfrowych reprezentacji (ang. *digital twins*) kolejnych obszarów świata rzeczywistego oraz czerpania wartości ekonomicznej, społecznej lub politycznej z pozyskanych w ten sposób informacji"[9]. Dane cyfrowe, które niemal z dokładnością zwierciadlanego odbicia opisują, odwzorowują i reprezentują otaczający nas świat, obiekty i wydarzenia, wprowadzają nas w rzeczywistość, którą David Gelernter nazwał „lustrzanymi światami" (ang. *mirror worlds*)[10]. Są nowym wymiarem ludzkiego życia bazującym na danych i zasilanym danymi, którego rozwój wymagał będzie „nowych rynków, instytucji, infrastruktury, przedsiębiorstw, a nawet ustaleń geopolitycznych"[11]. Ten cyfrowy wymiar rzeczywistości nie jest jedynie odwzorowaniem tego rzeczywistego, ale jest narzędziem i bytem coraz bardziej niezależnym, dopełniającym świat fizyczny. Dzięki światu cyfrowemu możliwe jest optymalizowanie procesów zachodzących w świecie fizycznym[12].

Aktualnie wolumen danych rośnie w tempie wykładniczym, co wynika z popularyzacji Internetu, większej przepustowości sieci oraz olbrzymiej liczby podłączonych do niej urządzeń. Ilość danych generowanych przez urządzenia w najbliższym czasie znacząco się zwiększy z uwagi na postępującą cyfryzację gospodarki w ramach czwartej rewolucji przemysłowej i tzw. drugiej fali danych – dane przemysłowe (ang. *industrial data*) stanowić będą nawet 90% wszystkich. Ilość danych wzrośnie także wraz z liczbą urządzeń składających się na tzw. Internet Rzeczy (ang. *Internet of Things*), która sięgnie 500 mld w 2030 r., oraz liczbę smartfonów, która szacowana jest na 8,5 mld w 2025 r.[13] W 2015 r. IBM wyliczył, że 90% danych na świecie zostało wytworzonych w przeciągu dwóch ostatnich lat, czyli od 2013 r.[14] W wyniku postępu technologicznego do 2025 r. każdego dnia na całym świecie będą tworzone, według szacunków, 463 eksabajty danych. W 2020 r. wolumen ten dla całego cyfrowego wszechświata osiągnie łącznie 44 zettabajty[15]. Dane cyfrowe stały się strategiczną wartością, kiedy dla platform cyfrowych i innych organizacji, w tym państw, zaczęły stanowić źródło tworzenia wartości i przewag konkurencyjnych. Nie jest bowiem istotna wyłącznie ilość generowanych cyfrowych danych, ale przede wszystkim **umiejętność wspinania się po łańcuchu wartości danych** (od zbierania surowych danych, poprzez ich składowanie, aż po analizę i przetworzenie w wysokiej jakości informacje, a następnie w wiedzę) oraz **monetyzacja danych**, które stały się nowym zasobem gospodarczym wpływającym na stosunki handlowe i rozwój gospodarczy globu**.** Proces ten przemodelowuje świat, zwiększając wagę i potęgę aktorów, którzy dostrzegają potrzebę strategicznego i systemowego podejścia do zbierania i wykorzystywania danych. Jest on kluczowy, dlatego że w najbliższych latach dane dosłownie zaleją rynek – *Big Data* staną się *even bigger*.

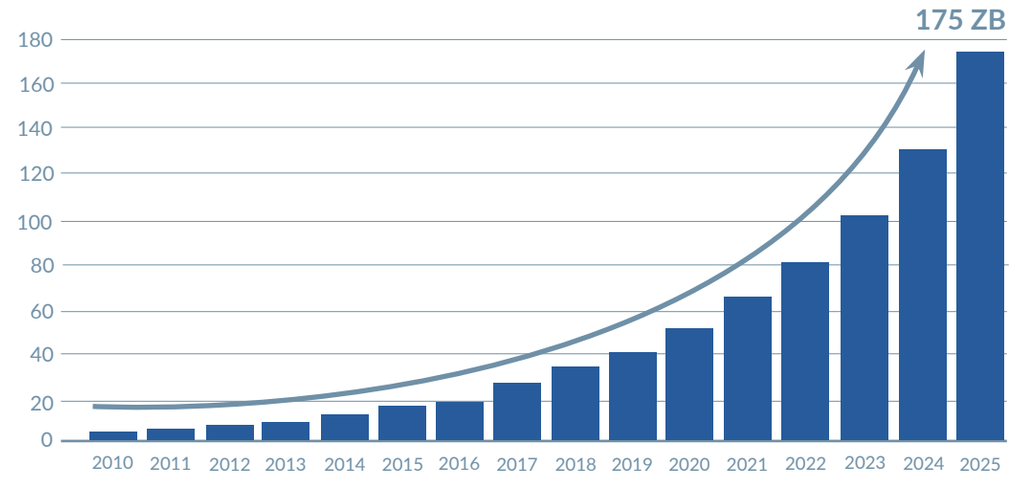
W świecie cyfrowym coraz większego znaczenia z punktu widzenia analizy geostrategicznej nabierają zatem mapy, które przedstawiają takie elementy jak ruch danych (z przewidywaną w okresie 2017–2022 największą, bo sięgającą 70%, koncentracją natężenia ruchu danych na świecie w regionie Azji i Pacyfiku oraz Północnej Ameryki), **układ infrastruktury** do ich transmisji (z naciskiem na podmorskie światłowody, które odpowiadają za 99% międzynarodowego przesyłu)[16], ale także **centra danych** (z których większość, bo 80%, zlokalizowana jest w krajach rozwiniętych, a 40% w USA)[17], czy też **lokalizację siedzib największych na świecie platform cyfrowych** (za 90% kapitalizacji rynku 70 największych platform odpowiadają firmy z USA i Chin).

Obraz, jaki płynie z analizy map cyfrowego świata, pokazuje dużą skupienie tego nowego ekonomicznego zasobu i infrastruktury w Chinach i USA. Kraje te stały się głównymi centrami grawitacji w nowym cyfrowym świecie i chcą czerpać największe korzyści geoekonomiczne w erze dominacji cyfrowych danych, które kapitalizować będzie można nie tylko w wymiarze ekonomicznym, ale także politycznym i militarnym.

Rodzaje danych:

- Dane osobowe i nieosobowe
- Dane prywatne i publiczne
- Dane do celów komercyjnych lub rządowych
- Dane wykorzystywane przez firmy, w tym korporacyjne dane, dane dotyczące zasobów ludzkich, dane techniczne i dane handlowe
- Dane nieustrukturyzowane i ustrukturyzowane
- Dane natychmiastowe i historyczne
- Dane dobrowolne, obserwowane i wywnioskowane
- Dane wrażliwe i niewrażliwe[18]

WYKRES 1.
WZROST WOLUMENU DANYCH NA ŚWIECIE



Roczny wolumen danych na świecie w zettabajtach (bilionach gigabajtów)

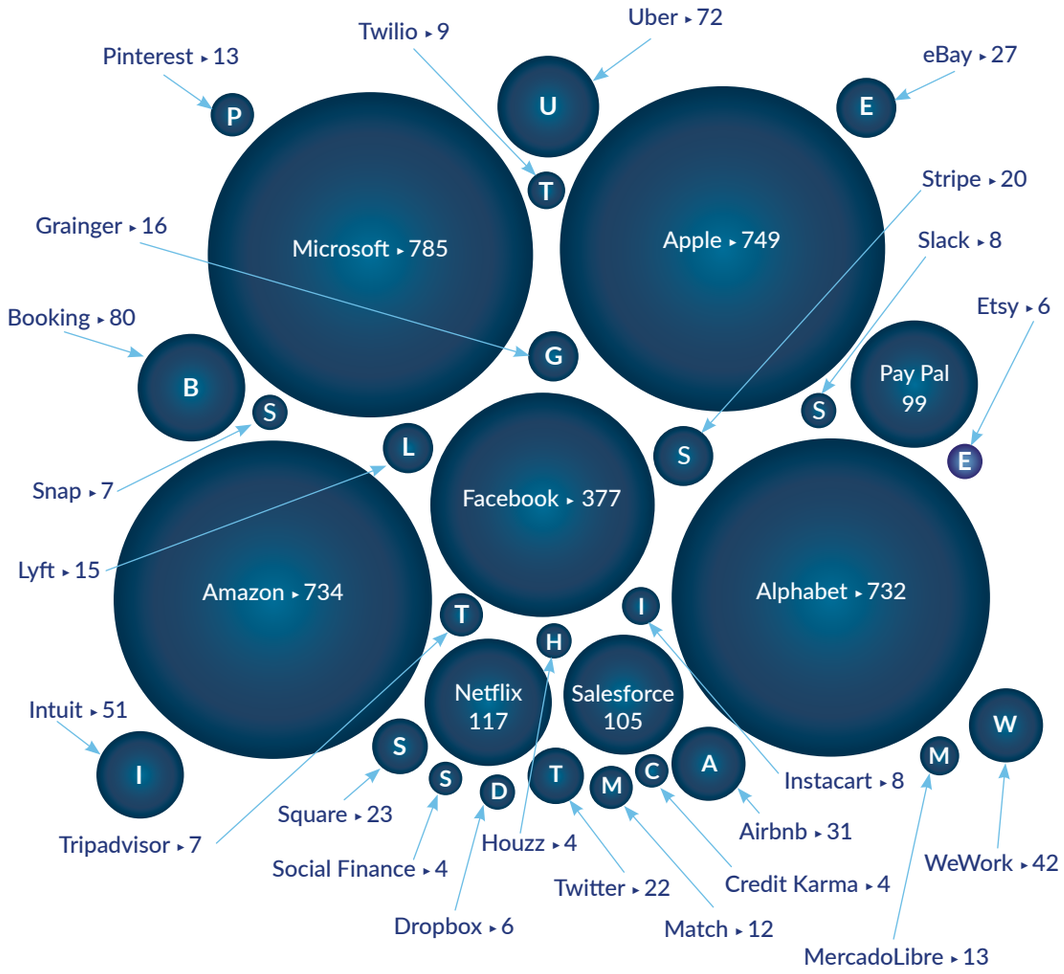
Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020, s. 65, na podstawie: Reinsel D., Gantz J., Rydning J., *The Digitization of the World. From Edge to Core*, 2018, s. 6

MAPA 1.

DYSTRYBUCJA GEOGRAFICZNA GŁÓWNYCH PLATFORM NA ŚWIECIE W 2018 ROKU

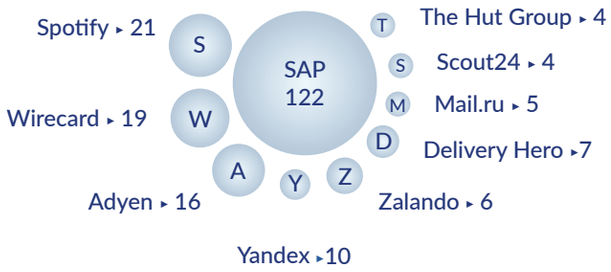
(KAPITALIZACJA W MILIARDACH DOLARÓW)

AMERYKA

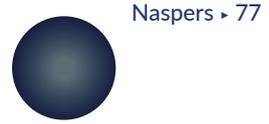


Udział w łącznej wartości

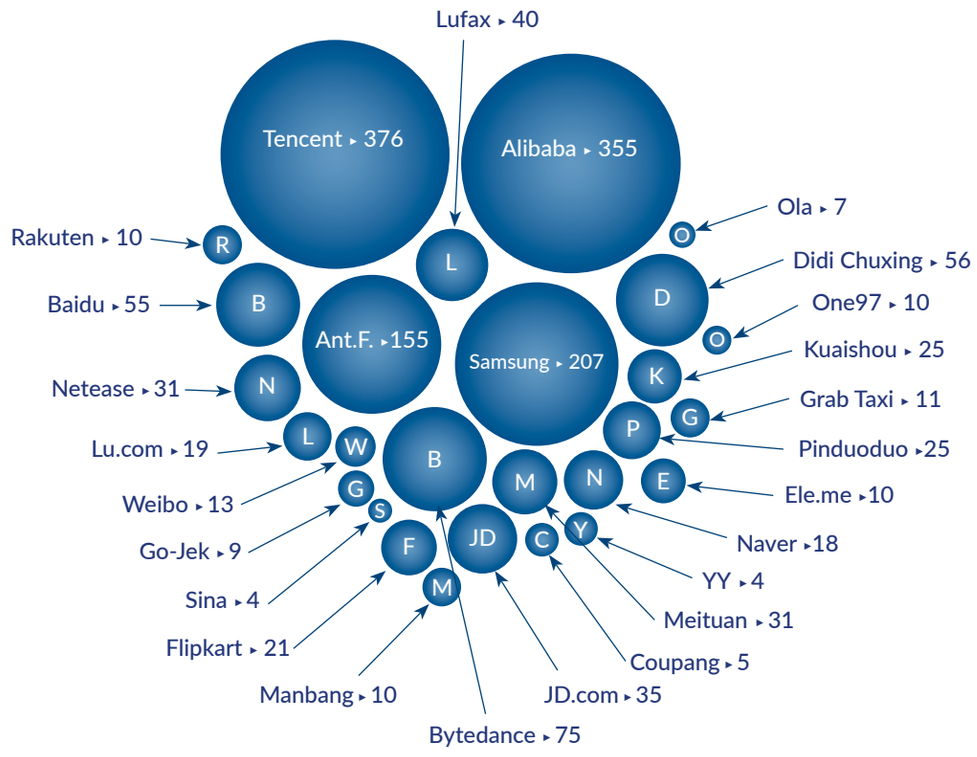
EUROPA



AFRYKA



AZJA



Źródło: *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. 10.

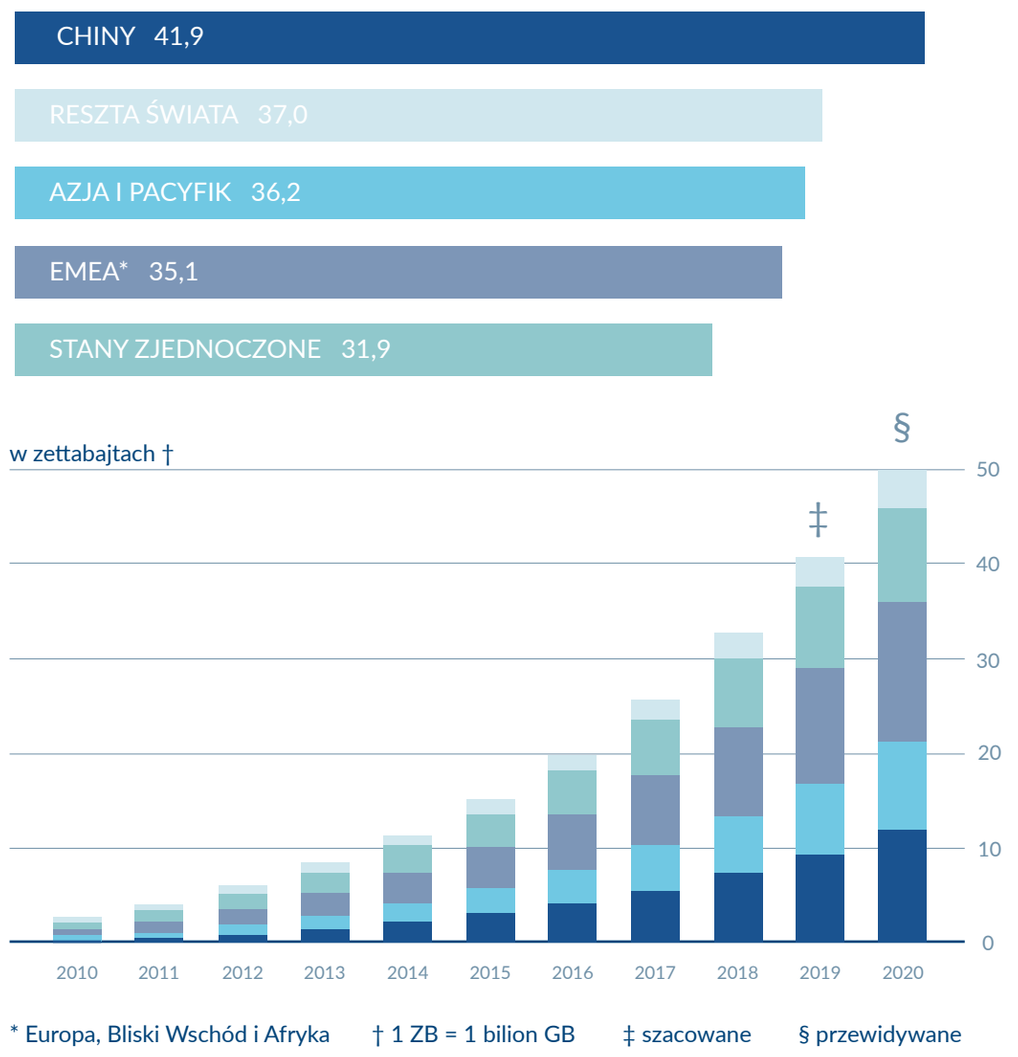
DANE A POZYCJA GEOEKONOMICZNA

W nowym cyfrowym świecie pozycja geoekonomiczna krajów zależeć będzie od skutecznej cyfrowej transformacji gospodarki po zapewnieniu odpowiednich do jej rozwoju warunków. Wymienić wśród nich należy m.in.: skuteczne i długofalowe strategie transformacji cyfrowej; wsparcie rozwoju infrastruktury cyfrowej; dostosowanie systemu edukacji do potrzeb i wyzwań cyfrowego świata; odpowiedni system instytucjonalno-prawny, sprzyjający rozwojowi ekosystemu innowacji opartych na danych oraz współpracę publiczno-prywatną, która odpowiednio zaprojektuje relacje z firmami technologicznymi[19].

Gospodarka cyfrowa, która składa się z **fundamentalnych innowacji technologicznych** (takich jak procesory i półprzewodniki), **podstawowych technologii** (komputery, urządzenia telekomunikacyjne) i **infrastruktury** (Internet, sieci telekomunikacyjne), a także **sektora ICT** (produkującego produkty i usługi, które polegają na kluczowych technologiach cyfrowych) i **sektorów cyfryzujących się** (w których produkty i usługi cyfrowe są coraz częściej wdrażane)[20], jest oparta przede wszystkim na danych. Rozwija się dynamicznie dzięki procesowi datafikacji z udziałem wielorakich źródeł danych, które napływają z systemów informatycznych, platform internetowych, aplikacji mobilnych, gdzie generowane są przez indywidualnych, biznesowych i instytucjonalnych użytkowników Internetu[21]. Mimo że źródła danych są różne, to aktualnie najcenniejszym są wciąż te, które generują indywidualni użytkownicy Internetu. Można zatem wysnuć wniosek, że im większa populacja danego kraju i odsetek obywateli z dostępem do Internetu, tym większe „naturalne" zasoby danych. Państwa posiadają jednak także inne wielkie zasoby danych publicznych, które przynajmniej częściowo starają się udostępniać w modelu Open Data. Zasobem publicznym o istotnej wartości i potencjale do tworzenia nowych produktów i usług są m.in. dane geoprzestrzenne, meteorologiczne, statystyczne, w tym np. dotyczące mobilności czy przedsiębiorstw i ich własności[22]. Kolejnym źródłem są dane z urządzeń ubieralnych (ang. *wearables*) oraz pozyskiwanych i agregowanych z przestrzeni publicznej oraz prywatnych urządzeń w wyniku coraz powszechniejszej „sensoryzacji" świata. Z uwagi na różnorodność danych, które składają się na zasób zwany *Big Data*, istotna jest umiejętność odpowiedniej integracji danych pozyskiwanych z różnych źródeł. Cyfrowa gospodarka rozwija się nie tylko w wyniku niczym nieograniczonego, a wręcz stymulowanego technologicznie i regulacyjnie przyrostu danych, ale także z powodu zwiększenia mocy obliczeniowych czy rozwoju usług w chmurze oraz algorytmów i technologii sztucznej inteligencji[23]. Najistotniejsze znaczenie ekonomiczne ma monetyzacja danych, czyli rola, jaką dane odgrywają w generowaniu przychodów platform cyfrowych (usługi reklamowe, *e-commerce*, platformy produktowe i chmurowe) i udziału tychże w PKB poszczególnych krajów oraz tworzeniu wartości, ale także optymalizacji procesów produkcyjnych[24]. Realną wartość danych krajowych (ang. *value of the country's data*) próbowała oszacować niedawno agencja rządowa Statistics Canada. W metodologii przyjęto, że na dane krajowe składają się dane znajdujące się „aktualne na stanie" oraz powiązane z nimi oprogramowanie i własność intelektualna. Wyliczenia wskazały, że wartość danych Kanady wynosi od 118 do 164 mld $. Z kolei analogicznie Stanów Zjednoczonych od 1,4 bln – 2 bln $, co stanowiłoby prawie 5% amerykańskich prywatnych zasobów kapitału fizycznego[25].

Dane są traktowane jak kapitał cyfrowego świata, często porównywany do ropy naftowej, stanowiący czynnik produkcji, który wpływa na efektywność, innowacyjność i relacje gospodarcze[26]. Biorąc pod uwagę cechy, jakie można im przypisać, bardziej zasadne jest także porównanie np. do powietrza: niezastępowalność (ang. *non-fungible*) z uwagi na unikalną wartość informacyjną pojedynczego zbioru; nierywalizacyjność (ang. *non-rivalry*) z uwagi na możliwość wykorzystania pojedynczego ich zbioru przez inne algorytmy i uzyskanie każdorazowo istotnej wartości rynkowej[27], replikowalność (ang. *replicability*) i możliwość ponownego użycia (ang. *reuse*).

WYKRES 2.
DANE GENEROWANE NA ŚWIECIE, ROCZNY ŚREDNI WZROST W LATACH 2010–2018



Źródło: *A deluge of data is giving rise to a new economy*, The Economist, za: IDC, Seagate, 20.08.2020, [online:] https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy

Coraz istotniejszy dla rozwoju cyfrowej gospodarki jest także trend innowacyjnych i transformujących zmian przeprowadzanych w oparciu o dane w procesie dostosowania starych modeli biznesowych i umacniania pozycji rynkowej przez firmy należące do tradycyjnych sektorów. Aktualną ilustracją tego procesu może być zainteresowanie amerykańskiego giganta sieci sprzedaży detalicznej, firmy Walmart, zakupem w partnerstwie z Microsoftem aplikacji mobilnej TikTok od chińskiej firmy ByteDance. Oprócz geopolitycznych powodów tej planowanej transakcji warto zwrócić także uwagę na jej aspekty, które wynikają z rosnącej wartości strategicznej dostępu do wielkich zasobów danych, generowanych na bieżąco i przez konkretne grupy konsumentów. Zakup TikToka może bowiem umożliwić Walmartowi lepsze dotarcie do młodzieży, zapewnić mu cenne dane na temat zachowań konsumentów w Internecie[28], a także uplasować w czołówce firm branży *in-video commerce*, rozwijającej się dzięki analizie danych i zastosowaniu sztucznej inteligencji. Jaka jest wartość rynkowa takich danych, pokaże cena ewentualnego zakupu TikToka.

W tym miejscu należy zwrócić uwagę na jeszcze jeden ważny trend, a mianowicie **kwestię własności danych** (ang. *data ownership*). W gospodarce opartej na danych duże zbiory danych są kluczowe dla modeli biznesowych i zysków firm. Coraz większa jest jednak świadomość tego, że firmy zbierające dane i zarządzające nimi nie tylko zarabiają na zagregowanych danych, głównie poprzez reklamy, ale często wymagają od użytkowników przekazania niektórych praw do nich w zamian za korzystanie z ich usług[29]. Problem pogłębiają nieodłączne obaw o bezpieczeństwo danych użytkowników. W związku z tym pojawiają się pytania dotyczące własności danych i stworzenia użytkownikom szansy, by nie tylko korzystali z usług platformy, ale również korzystali na danych, które dostarczają. W tym wymiarze podejścia koncentrują się na wynagradzaniu osób, które udostępniają dane platformom internetowym bezpośrednio oraz za pośrednictwem trustów danych. Choć ustalenie wartości zagregowanych danych jest możliwe (o czym świadczy przykład Statistics Canada), pojawia się jednak problem braku prostego sposobu wyceny danych za jednostkę, przez co rekompensata dla użytkowników wydaje się niezwykle trudna do wyliczenia[30]. Nawet biorąc pod uwagę, że istniałoby narzędzie stworzone przez rynek, zdolne oceniać poszczególne fragmenty danych, które tworzą użytkownicy, pojawia się pytanie, kto i jak powinien rozstrzygać ten proces[31]. Z tego względu eksperci wskazują także, że dane można charakteryzować i postrzegać jako **dobro publiczne** (ang. *public good*), które należy wykorzystywać w sposób, który maksymalizowałby zrównoważone tworzenie dobrobytu w społeczeństwie, ale także skutkowałby wzrostem wydajności i produktywności. Jednym z pojawiających się trendów w tym obszarze są **koncepcje demokratyzacji danych i inicjatywy otwartych danych**[32]. Jest to spójne z koncepcją zbiorowej własności danych i funduszy danych cyfrowych jako podstawy dla ich nowego zbioru opartego na otwartych licencjach (ang. *digital data commons*), jak ma to miejsce np. w przypadku Creative Commons[33].

Zatem w procesie budowy cyfrowej gospodarki obserwować będziemy także dyskusje i różne podejścia krajowe do procesu zapewniania powszechnego, pozbawionego barier dostępu do danych nie tylko na poziomie państw i firm, ale także indywidualnych internautów. Z pewnością konieczne będzie podejście eksperymentalne, uwzględniające różne opcje, i ocena zarówno ich wykonalności, jak i zalet oraz wad[34].

DANE A POZYCJA „GEOTECHNOLOGICZNA"

Z pozycją geoekonomiczną wiąże się ściśle zdolność państwa do projekcji siły i budowania przewag, która wynika z możliwości kontroli wytwarzania rozwiązań technologicznych. Uznać można, że jest to pozycja „geotechnologiczna"[a].

a Mowa tu o znaczeniu słowa „geotechnologia", którego użył Stephen Robert Nagy, określając ją jako wpływ technologii na projekcję siły i budowanie przewag geopolitycznych i geoekonomicznych przez państwa, Por. Nagy S. R., *Geotechnology meets geopolitics: US-China AI Rivalry and Implication for Trade and Security*, World Commerce Review, 2018.

Zatem dla rozwoju gospodarki cyfrowej i generowania wartości istotny jest rozwój rodzimego sektora ICT, czyli gałęzi przemysłu skupiającej się na „elektronicznym przetwarzaniu, przekazywaniu oraz prezentowaniu danych i informacji"[35]. Kraje powinny dążyć do znaczącego udziału tego sektora w krajowym PKB i eksporcie. Jak omówiono w rozdziale drugim, w tym obszarze dominują przede wszystkim dwa kraje, które są siedzibami globalnych firm technologicznych, Stany Zjednoczone (Microsoft, Alphabet, Apple, Amazon, Facebook) i Chiny (Tencent, Alibaba, Baidu, JD, ByteDance). To umiejętność generowania wartości z danych decyduje o ich pozycji konkurencyjnej na rynku, a wartość rynkowa wymienionych firm opiera się przede wszystkim na zasobach niematerialnych, do których należą dane, wykorzystywane przez te firmy w modelach biznesowych, w znacznie mniejszym stopniu przychody generowane są natomiast przez zasoby twarde[36]. Dane są także źródłem informacji i wiedzy o rynku oraz konsumentach, klientach i użytkownikach.

Dlatego ważne jest wspieranie przez państwo rozwoju krajowej branży ICT. Wzrost gospodarczy w oparciu o sektor ICT oraz optymalizację wykorzystania danych będzie szczególnie ważnym źródłem odbicia się gospodarek po pandemii COVID-19[37].

DANE A POZYCJA GEOPOLITYCZNA

W wymiarze geopolitycznym dostęp do danych wpływa na możliwość projekcji *soft* i *hard power* (temat tych interferencji opisany został w rozdziale drugim), a także buduje potęgę polityczną i militarną krajów.

W pierwszej kolejności zwrócić trzeba uwagę, że dane są zasobem, który rozwija „potęgę informacyjną" (ang. *information power*) państwa. Informacja od zawsze była, jest i będzie atrybutem i instrumentem składającym się na siłę państwa projektowaną do wewnątrz i na zewnątrz, z potencjałem konsekwencji geopolitycznych, dlatego w skali świata trwa o nią współzawodnictwo. Rola informacji aktualnie rośnie w związku z postępami technologii cyfrowych opartych na danych (ang. *data-driven technologies*)[38] i penetracją przez nie naszej rzeczywistości. Z kolei w wymiarze walki na narracje wzmacnia się w związku z rozwojem platform mediów społecznościowych, które opierają się na zbieraniu i analizie danych, ale są także ich istotnym źródłem (ang. *data-driven social media*). Nie bez powodu Chiny i Rosja wierzą, że strategiczna rywalizacja w XXI wieku będzie „zero-jedynkowym pojedynkiem o kontrolę nad cyfrowymi danymi", *nomen omen* zapisanymi zero-jedynkowym kodem binarnym, ale także o „technologię oraz zasoby ludzkie, dzięki którym możliwa jest konwersja danych na cenne informacje"[39]. Ochrona danych generowanych w kraju, a dotyczących opinii i preferencji obywateli, jest postrzegana jako budowanie odporności na działania dezinformacyjne, dlatego że adwersarze w oparciu o te dane budują sprofilowane komunikaty i narracje, aby siać chaos informacyjny, polaryzować i radykalizować społeczeństwa czy wpływać na procesy demokratyczne, co prowadzi nawet do wojen dyplomatycznych. W tym wymiarze dane są używane do projekcji *soft power*, ale także jako broń (ang. *weaponization of information*). W filmie dokumentalnym *Hakowanie świata* w reżyserii Karima Amera i Jehane Noujaim pada nawet stwierdzenie, że psychografia, czyli metodologia jakościowa używana do opisywania konsumentów na podstawie cech charakteru, która stosowana jest przez algorytmy niektórych platform internetowych powinna zostać sklasyfikowana jako taktyka komunikacyjna o statusie broni (ang. *weapons-grade communication tactics*). Jak zauważa raport NATO Science & Technology Organization, media społecznościowe wielokrotnie zostały zaprzęgnięte do mobilizacji ludności i osiągnięcia celów politycznych i społecznych, a gromadzenie danych pozwala na zrozumienie ludzkich zachowań społecznych i dynamiki grupowej na niespotykaną dotąd skalę[40]. Dlatego NATO zalicza fake newsy i dezinformację do kategorii nasilających się zagrożeń wojny cyfrowej (ang. *emerging digital warfare threats*) oraz buduje zaawansowane zdolności i narzędzia analityczne do analizy danych w czasie rzeczywistym,

która ułatwi podejmowanie decyzji (więcej o tym temacie w rozdziale trzynastym). Dla zdyskontowania danych, zarówno biznesowego, jak i politycznego, istotne znaczenie ma zatem przede wszystkim umiejętność ich przetworzenia dzięki analizie na informacje i wiedzę, co prowadzi do konieczności rozwijania przez państwa i organizacje coraz lepszych technik i narzędzi analitycznych[41].

W świecie opartym na danych cyfrowych budowanie **potęgi politycznej** zależeć będzie także od właściwego wykorzystania danych na potrzeby poprawy procesów zarządzania państwem i sprawności procesu decyzyjnego, a także oszczędności budżetowych i zrozumienia trendów.

W kontekście budowy przewag politycznych i militarnych istotne znaczenie ma także zastosowanie danych na potrzeby działań służb wywiadowczych. Od kilku dekad dzięki postępom techniki ten obszar działalności państw przechodzi rewolucję, którą dodatkowo pogłębia rosnąca ilość danych pochodzących z systemów telekomunikacyjnych, dronów, satelitów, kamer przemysłowych czy różnego rodzaju sensorów, do których dotrzeć mogą agencje wywiadowcze. Dane te przetworzone z pomocą sztucznej inteligencji znacznie pogłębią możliwość operacyjnej analizy w ramach SIGINT (ang. *Signals Intelligence*)[42] oraz GEOINT (ang. *Geospecial Intelligence*)[43]. Z uwagi na ilość danych pozostawianych w Internecie oraz ich wycieki rosną także zdolności OSINT (ang. *Open Source Intelligence*), czyli białego wywiadu, polegające na zdobywaniu informacji na temat ludzi oraz organizacji z ogólnodostępnych źródeł, a następnie ich analizie nowymi zaawansowanymi technologicznie metodami. Spadać natomiast zacznie rola HUMINT (ang. *Human Intelligence*), czyli rozpoznania osobowego, gdyż źródła osobowe mogą zostać z powodzeniem zastąpione przez „źródła IT", które „wejdą" w posiadanie naszych danych i w konsekwencji informacji o nas. To maszyny i urządzenia, które posiadać będą ludzie, dostarczą wystarczającej informacji o ludzkich zachowaniach, a nawet intencjach – ale także maszyny będą szpiegować maszyny, bo to one będą coraz częściej podejmować ważne decyzje i autonomiczne działania. Autonomiczne systemy staną się zatem celami wywiadowczymi, i całkiem możliwe, że prowadzonymi wobec nich przez maszyny, co *de facto* oznacza, że wywiad oraz kontrwywiad będzie mógł się odbywać bez ludzkiego udziału i interwencji[44]. Strategiczne znaczenie dostępu do danych, umiejętności ich analizy oraz weryfikacji jest zatem ogromne. Państwa, których agencje wywiadowcze zdobędą zdolności szybkiego pozyskiwania i przetwarzania ogromnych mas złożonych danych ze wszystkich dostępnych źródeł – czyli *de facto* zintegrują wszystkie wymienione formy działalności wywiadowczej – będą miały przewagę nad tymi, które tego nie będą potrafić[45]. Dotyczy to nie tylko zastosowania informacji wywiadowczych do sfery cywilnej, ale także militarnej.

Charakteryzując znaczenie danych dla **potęgi militarnej**, warto zwrócić uwagę na fakt, że NATO uznało analizę wielkich zbiorów danych (ang. *Big Data and Advanced Analytics* – BDAA) za jeden z priorytetów dostosowania sojuszu do wyzwań cyfrowego świata. Duże zbiory danych i ich analityka umożliwiają prognozowanie, wspomaganie podejmowania decyzji w czasie rzeczywistym i wyróżnianie wczesnych wskaźników sukcesu i kryzysu[46]. Dlatego NATO zwraca uwagę, że wiele krajów członkowskich dokonało już znacznych inwestycji w BDAA, zarówno w środowiskach cywilnych, jak i wojskowych, co pozwoli sojuszowi czerpać z tych inwestycji, jednocześnie je rozszerzając, dostosowując i integrując w procesach i operacjach NATO[47]. W wymiarze rywalizacji geopolitycznej sytuację doskonale scharakteryzował Jens Stoltenberg, mówiąc na NATO Industry Forum w Waszyngtonie w 2019 r., że Chiny poprzez „stawanie się światowym liderem w rozwoju różnych przełomowych technologii, od rozpoznawania twarzy po obliczenia kwantowe, są w stanie zebrać ogromne ilości danych nie tylko z Chin, ale z całego świata, w tym z krajów sojuszniczych NATO"[48]. Aby sprostać rosnącym potrzebom w zakresie analityki danych, konieczne będą ciągłe inwestycje w zwiększanie możliwości w tym zakresie, współpracę badawczo-rozwojową i wspólne

standardy, a także polityki gromadzenia, przechowywania i zarządzania danymi, które zapewnić powinny docelową pomyślną integrację BDAA w operacje sojuszu i jego codzienne funkcjonowanie[49]. Jednocześnie rozważania dotyczące danych cyfrowych mają zastosowanie w dyskusji o ich przechowywaniu i konieczności zapewnienia bezpieczeństwa i integralności z uwagi nie tylko na ich znaczenie dla operacji militarnych czy też procesu podejmowania w przyszłości decyzji, ale także na sytuację, w której NATO nie miałoby dostępu do swojej fizycznej siedziby[50]. Przez konieczność zapewnienia bezpieczeństwa danych generowanych przez NATO są one przesyłane dedykowanymi sieciami, przechowywane w specjalnie stworzonej chmurze i wykorzystywane w aplikacjach istotnych z punktu widzenia Sojuszu. NATO pracuje nad utworzeniem własnego Data Science Centre, które będzie wykorzystywało dane, by sprostać wyzwaniom XXI wieku[51]. Sojusz podkreśla również potrzebę rozwijania na terytorium Sojuszu godnych zaufania sieci telekomunikacyjnych, którymi transferowane są dane, wskazując, że różnice krajów sojuszniczych w podejściu do zagrożeń z tym związanych i rozwój niekompatybilnych systemów może zmniejszyć możliwości dzielenia się wrażliwymi danymi oraz współpracy systemów C4ISR (ang. *Command*, *Control*, *Communications*, *Computers*, *Intelligence*, *Surveillance*)[52]. Eksploatacja danych cyfrowych jest uznawana za krytyczną przewagę nad przeciwnikami i ich siłami, a zdolność do wykorzystania tych zasobów przez siły wojskowe ma coraz istotniejsze znaczenie dla skuteczności działań operacyjnych. Umiejętność natychmiastowego gromadzenia danych i informacji dzięki nowoczesnemu sprzętowi i urządzeniom może ułatwić podejmowanie zarówno decyzji strategicznych, jak i decyzji „w terenie". Prawdziwym testem dostosowania do zmieniających się uwarunkowań technologicznych w zakresie zdolności oraz działań obronnych i militarnych będzie użycie danych w rozwiązaniach opartych na sztucznej inteligencji. Znaczenie danych dla bezpieczeństwa narodowego rośnie bowiem wraz z rozwojem tejże technologii i jej zastosowaniem w obszarze militarnym (co opisano w rozdziale dziesiątym). Wśród wielu innych wojskowych zastosowań analityki danych można podać trend *digital twins*, który pomoże w bardziej wydajnym zarządzaniu cyklem życia aktywów militarnych i sprzętu wojskowego oraz prowadzeniu operacji bojowych[53]. W czasie operacji militarnych coraz większe znaczenie ma też analiza w czasie rzeczywistym pozyskanych danych wywiadowczych (ang. *intelligence*), co zwiększa świadomość sytuacyjną.

JAK KRAJE RYWALIZUJĄ O DANE?

Proliferacji danych oraz wzrostowi ich znaczenia dla pozycji geoekonomicznej i geopolitycznej państw od lat towarzyszy rosnąca liczba cyberataków i zagrożeń dla prywatności danych, a przede wszystkim dynamiczny rozwój rywalizacji o nie. Cztery lata temu Bruce Schneier zatytułował swoją sławną książkę *Dane i Goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem*. W 2020 r. zawartość książki nie straciła na aktualności, ale z pewnością bitwa, o której mowa, jest coraz mniej „ukryta". Jej uczestnikami są nie tylko firmy technologiczne, wykorzystujące coraz to nowsze zdobycze technologiczne do generowania wartości z danych, ale przede wszystkim państwa. Poszczególne kraje oraz grupy krajów (np. UE) starają się chronić dane generowane przez swoich obywateli oraz wspierać krajowe firmy technologiczne w realizacji strategii biznesowych. Naocznie obserwujemy coraz aktywniejsze działania państw nakierowane na ograniczenie podmiotom zewnętrznym zakresu pozyskiwania danych ich obywateli oraz informacji generowanych w obrębie własnych granic, co świadczy o wzroście świadomości znaczenia danych. Na szali jest aktualnie swobodny dostęp do globalnego Internetu oraz transfer i przetwarzanie danych.

1. „Bałkanizacja Internetu"

Idea podziału Internetu, znana jako jego „bałkanizacja", „cyberbałkanizacja" lub *Splinternet*, rozwijała się na przestrzeni ostatnich lat[b] i odnosi

b Neologizm ten po raz pierwszy użyty został w 1996 r. przez naukowców MIT – Marshalla Van Alstyne'a oraz

się do fragmentacji globalnego Internetu na kilka mniejszych, administrowanych na szczeblu krajowym sieci internetowych, podzielonych wzdłuż granic politycznych[54]. Obawy o nią wynikały często z braku regulacji w zakresie globalnego zarządzania Internetem lub też z obawy o złe regulacje połączone z dużą centralizacją procesu decyzyjnego[55]. Cyberbałkanizacja, którą obserwujemy obecnie, ma swoje źródło w powolnych zmianach geopolitycznych, które wiążą się z utratą przez USA pozycji jedynego globalnego supermocarstwa na korzyść aspirującej do uzyskania światowej pozycji ChRL i jej próbami odejścia od amerykańskocentrycznej architektury Internetu. Tworzące się granice Internetu odzwierciedlają również największe międzynarodowe napięcia i konflikty, które rozgrywają się w świecie rzeczywistym. Działania na największą skalę podejmują obok Chin inne kraje, które mają sprzeczne z USA interesy geopolityczne, m.in. Rosja, Korea Północna czy Iran. Cyberbałkanizacja zawdzięcza swoją aktualną dynamikę także rosnącej roli – geokonomicznej i geopolitycznej – danych cyfrowych oraz próbom ich zatrzymania na terytorium poszczególnych krajów. Dalszy brak konsensusu i współpracy w tematach cyfrowych może, w połączeniu z rywalizacją technologiczną mocarstw, doprowadzić do powstania „żelaznych" granic cyfrowych, które nie tylko zahamują przepływ danych i informacji, ale pogłębią trwający równolegle proces rozrywania cyfrowych łańcuchów dostaw (ang. *decoupling of digital supply chains*) i zahamują inwestycje transgraniczne.

Chiny są krajem, któremy w stopniu najbardziej zaawansowanym oddzielił się od usług internetowych i telekomunikacyjnych zdominowanych przez amerykańskie firmy. ChRL, która podejmowała działania związane z kontrolą Internetu od 1997 r., jest na ten moment krajem najbardziej posuniętym w kierunku cyberbałkanizacji[56]. Odizolowany **Wielkim Firewallem** (ang. *The Great Firewall of China*, chiń. 防火长城) chiński internet, oficjalnie uruchomiony w 2002 r., pozwala Komunistycznej Partii Chin całkowicie monitorować wszelką działalność *online* obywateli i wdrożyć zaawansowany system filtrowania i cenzury, który uniemożliwia im dostęp do treści i usług będących w ocenie Partii szkodliwymi i niebezpiecznymi, w tym wyszukiwarki Google i portali takich jak Facebook, Twitter, Wikipedia. Dzięki kontroli internetu, danych i informacji utrzymywana jest ścisła kontrola społeczna, a także budowana suwerenność cyfrowa ChRL. Procesowi temu towarzyszy jednoczesny globalny sukces rynkowy chińskich firm technologicznych, które aktualnie, podobnie jak amerykańscy giganci, świadczą usługi i sprzedają produkty nie tylko swoim obywatelom, ale też użytkownikom w innych krajach. Chińskie wysiłki miały potężny efekt demonstracyjny, pokazujący innym autokratom, że Internet można skutecznie kontrolować[57]. Korea Północna uruchomiła krajowy internet, tzw. **Kwangmyong** (dosłownie „jasne światło"), w 2000 r., a Iran w 2011 r. swoją **Narodową Sieć Informacyjną** (określaną też jako krajowy intranet i Internet halal). Do grona autorytarnych władców z własną siecią ostatnio dołączył także Władimir Putin, podpisując w 2019 r. ustawę *Sovereign Internet Bill*, która ustanowiła samowystarczalny internet o nazwie **RuNet**. W ramach tych działań Rosja zmusza wszystkich dostawców usług w sieci do przechowywania danych w kraju i już zapowiedziała, że przygotowała system, który pozwoli jej całkowicie odłączyć się od Internetu. Jest to tzw. opcja „wyłącznika awaryjnego" (ang. *kill switch*), który odłącza rosyjskich użytkowników od globalnej sieci. Rosja chce kierować ruch internetowy i ruch danych w kraju przez punkty, które kontroluje państwo, zmniejszając zależność od zagranicznych serwerów, nad którymi nie ma pożądanej kontroli[58]. Oficjalnie zabieg ten ma natomiast chronić rosyjską cyberprzestrzeń przed atakami z zagranicy.

Erika Brynjolfssona, a spopularyzowany został w 2002 r. przez Clyde'a Wayne'a Crewsa, badacza z Cato Institute. Zjawisko to dostrzega także m.in. Scott Malcomson, nazywając je terytorializacją Internetu (ang. *territorialization of the internet*).

GRAFIKA 1.

REGULACJE ZWIĄZANE Z LOKALIZACJĄ DANYCH

Chińskie prawo o cyberbezpieczeństwie i chmurze obliczeniowej wymaga, by informacje o obywatelach Chin albo związane z bezpieczeństwem państwowym przechowywano na krajowych serwerach. Przepisy zmusiły firmę Apple do przekazania miejscowej firmie danych chińskich obywateli ze swojej chmury, a Amazon do sprzedania prowadzonego centrum danych, aby podporządkować się nowym regulacjom w 2017 r.

Rosja może nakładać wysokie kary za nieprzestrzeganie zasady lokalizacji danych osobowych obywateli rosyjskich. Kraj ten przeprowadził udane testy własnego „samowystarczalnego, odłączonego internetu" zwanego RuNet.

Iran stworzył swój internet halal, oficjalnie określany jako Narodowa Sieć Informacyjna, licząca ok. 500 zatwierdzonych przez rząd krajowych stron, zapewniająca wyższe prędkości i niższe ceny korzystającym z niej odbiorcom.

Północnokoreańska wersja krajowego intranetu jest znana pod nazwą Kwangmyong, a zawiera sklepy online, strony randkowe, wiadomości itd

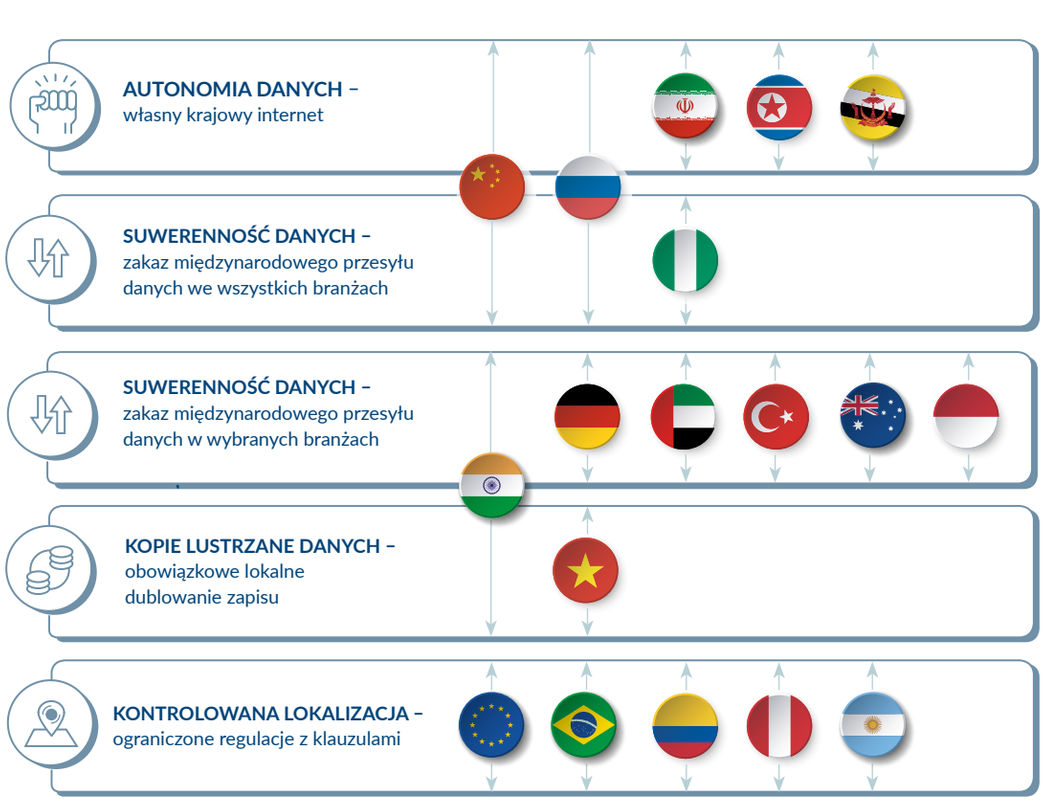
Źródło: Delta Partners Group[59]

Trudno ocenić, jakie skutki może mieć postępująca bałkanizacja Internetu, w tym jaki będzie jej wpływ na rozwój innowacji technologicznych i pozycję geopolityczną poszczególnych krajów. Założyć jednak należy, że samo ograniczenie przepływu danych miałoby z pewnością negatywne konsekwencje ekonomiczne. Posłużyć się można w tej prognozie kosztami tzw. celowego odcięcia Internetu (ang. *Internet shutdown*) w wielu krajach, które globalnie sięgnęły w 2019 r. 8 mld $[60]. Jest to coraz powszechniejsza praktyka rządów, gdyż co najmniej jedna czwarta krajów na świecie tymczasowo wyłączyła Internet w ciągu ostatnich czterech lat[61]. Obok skutków ekonomicznych możemy mówić także o skutkach geopolitycznych odcięcia Internetu. Niedawnym ich przykładem są wydarzenia wokół sfałszowanych wyników wyborów prezydenckich na Białorusi[62]. Spodziewać się należy negatywnych skutków dalszej cyberbałkanizacji dla przesyłania danych i informacji ponad granicami, współpracy międzynarodowej i wolności słowa w skali globalnej.

2. Strategie, polityki, regulacje

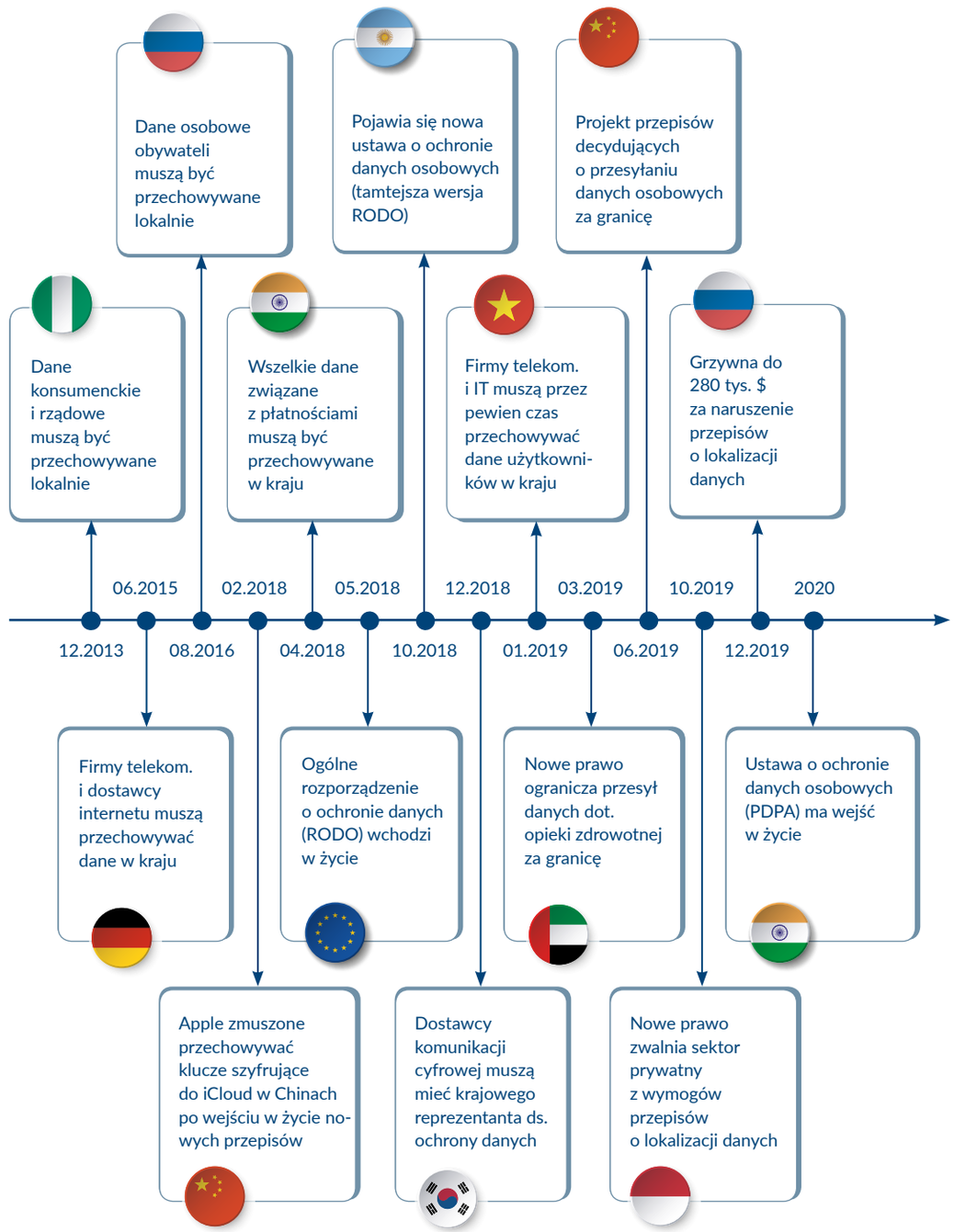
Obok „twardych działań", skutkujących rzeczywistymi i infrastrukturalnymi zmianami globalnego Internetu, wiele państw na świecie decyduje się na działania „miękkie" i regulacyjne mające budować suwerenność i autonomię danych. W wymiarze regulacyjnym kraje przyjmują coraz częściej **przepisy dotyczące lokalizacji danych** (ang. *data localisation laws*), które mają na celu kontrolę ich swobodnego przepływu, lub podejmują bardziej **umiarkowane działania w zakresie ochrony danych osobowych**. Prawo dotyczące lokalizacji danych wprowadza obowiązek gromadzenia, przetwarzania lub przechowywania danych o obywatelach lub rezydentach danego kraju w jego granicach terytorialnych, i zwykle ich przekazanie za granicę może nastąpić tylko po spełnieniu lokalnych wymogów dotyczących prywatności lub ochrony danych[63]. Jako argumenty przemawiające za wprowadzeniem tego prawa wymienia się nie tylko **względy geopolityczne** związane z bezpieczeństwem narodowym i interesem organów ścigania oraz prywatnością danych o obywatelach, **ale także ekonomiczne**. Lepsze możliwości zabezpieczenia danych przed atakami hakerskimi oznaczają ograniczenie strat finansowych związanych z ich utratą, a działania na rzecz protekcjonizmu gospodarczego postrzegane są jako środek wsparcia dla lokalnego biznesu ICT.

GRAFIKA 2.
REGULACJE ZWIĄZANE Z LOKALIZACJĄ DANYCH MAJĄCE NA CELU AUTONOMIĘ DANYCH



Źródło: Delta Partners Group[64]

GRAFIKA 3.
RÓŻNE POZIOMY REGULACJI DOTYCZĄCYCH LOKALIZACJI DANYCH



Źródło: Delta Partners Group[65]

Mniej inwazyjne regulacje, które w jednym ze swych wymiarów również regulują kwestie lokalizacji danych, dotyczą ochrony danych osobowych. W tym zakresie pionierem była Unia Europejska – w maju 2018 r. jej kraje członkowskie obowiązywać zaczęło rozporządzenie General Data Protection Regulation (GDPR)[c]. Umożliwia ono przesyłanie danych do innych krajów pod pewnymi warunkami, np. dane mogą być przekazywane tylko do tych krajów, które mają co najmniej taki sam poziom ochrony danych osobowych jak UE[66]. Przepisy na ten temat zostały przyjęte m.in. w Brazylii (port. Lei Geral de Proteção de Dados Pessoais), Indiach (ang. Personal Data Protection Bill), Korei Południowej (kor. 개인정보 보호법; ang. *Personal Information Protection Act*, PIPA). Podobne działania podejmowane są także w USA, gdzie w styczniu 2020 r. zaczął obowiązywać California Consumer Privacy Act, ale wiele innych amerykańskich stanów (Maine, Nevada, Waszyngton, Nowy Jork) ogłosiło zamiar przyjęcia własnych przepisów dotyczących prywatności danych. Problem systemu federacyjnego polega jednak na tym, że poszczególne przepisy stanowe mogą nie być ze sobą spójne. Dlatego coraz częściej pojawiają się głosy wzywające Kongres do przyjęcia w interesie narodowym „jednego, silnego, krajowego standardu ochrony prywatności"[67].

Innym przykładem rozwiązań legislacyjnych mających chronić dane są np. te podejmowane przez rosyjskie władze, gdzie w maju 2019 r. zaproponowano ustawę ograniczającą zagraniczną własność w firmach posiadających „znaczące zasoby informacyjne"[68]. Propozycja ta wstrząsnęła w szczególności akcjami największego w Rosji konglomeratu technologicznego Yandex, z uwagi na krążące pogłoski, że Kreml dąży do bardziej bezpośredniej kontroli nad firmą, aby mieć nadzór nad przekazywaniem danych osobowych rosyjskich użytkowników firmom zagranicznym. Tego typu działania zdaniem włodarzy na Kremlu mają wpływ na „narodowe interesy Rosji"[69]. Ostatecznie ustanowiona została fundacja powiązana z rządem, która posiada prawo weta w zakresie istotnych transakcji, w tym obejmujących „transfer danych rosyjskich użytkowników"[70].

Swobodny przepływ danych ma zasadnicze znaczenie dla rozwoju gospodarki cyfrowej, co sprawia, że egzekwowanie lokalizacji danych w poszczególnych krajach może być wąskim gardłem dla niektórych internetowych usług i cyfrowych branż[71] i z pewnością będzie miało wpływ na przyszłość cyfrowego świata, w tym rywalizację geoekonomiczną.

Wydaje się jednak, że aby odpowiedzieć na wyzwanie geopolityczne i geoekonomiczne związane z rolą i znaczeniem danych i informacji, konieczne są nie tylko wyrywkowe regulacje, ale stworzenie narodowych strategii, w tym regulujących status prawny danych, sposoby dzielenia się nimi wewnątrz i na zewnątrz kraju. Także w tym obszarze UE stała się jednym z globalnych pionierów. 9 lutego 2020 r. Komisja Europejska, wychodząc z założenia, że dane są siłą napędową rozwoju gospodarczego opublikowała europejską strategię w zakresie danych (ang. European Data Strategy). Przewiduje ona stworzenie jednolitego rynku danych oraz wspólnych europejskich przestrzeni danych w kluczowych z punktu widzenia rozwoju gospodarki sektorach. Dokument postuluje także wprowadzenie jasnych i przejrzystych reguł, które umożliwią swobodny przepływ i wymianę danych z poszanowaniem europejskich praw i wartości[72]. Koncepcja ta łączy się z obawami o charakterze geoekonomicznym i geopolitycznym, które kanclerz Niemiec Angela Merkel ujęła w ten sposób: „tak wiele firm europejskich po prostu przekazało wszystkie swoje dane firmom amerykańskim. […] Produkty o wartości dodanej, które się w rezultacie tego pojawią z pomocą sztucznej inteligencji, stworzą zależności, co do których nie jestem pewna, że są dobre"[73]. Z obawy tej oprócz wspomnianej strategii wynikają także inne działania, które w całym łańcuchu wartości danych mają zwiększyć kontrolę nad nimi przez europejskie podmioty. Równoległym działaniem jest bowiem uruchomienie europejskiej inicjatywy chmury obliczeniowej, projektu GAIA-X, którą Angela Merkel określiła jako „konkurencyjną, bezpieczną i godną zaufania infrastrukturę danych dla Europy"[74] (więcej o znaczeniu takiej infrastruktury w rozdziale szóstym). Wszystkie te regulacyjne i polityczne ruchy wokół danych wpisują się w dążenie do uzyskania przez UE cyfrowej autonomii. Peter Altmaier, minister gospodarki Niemiec, powiedział, że dane firm takich jak Volkswagen, ale także niemieckiego ministerstwa spraw wewnętrznych czy systemu ubezpieczeń społecznych, są coraz częściej przechowywane na serwerach amerykańskich, co w jego przekonaniu prowadzi do „utraty części naszej suwerenności". Komisja Europejska prognozuje, że do 2025 r. znacznie wzrośnie ilość danych przemysłowych i generowanych przez urządzenia Internetu Rzeczy, a ponieważ w tych obszarach UE aktywnie się rozwija, spodziewać się można ogromnego napływu rodzimych danych i wynikającej z tego procesu szansy dla europejskiej gospodarki, w szczególności MŚP[75].

Strategiczny namysł nad zasobami danych podejmuje teraz właśnie także ChRL, której władze opracowały bardzo ambitny i ciekawy metodologicznie projekt ustawy o nazwie Data Security Law[76], który był poddawany konsultacjom do 16 sierpnia 2020 r. Ustawa zakłada utworzenie systemu klasyfikacji danych na poziomie krajowym, który określałby różne ich rodzaje w zależności m.in. od wpływu na bezpieczeństwo narodowe, interes publiczny czy stopień ważności dla rozwoju gospodarczego, a od oceny uzależniony byłby stopień ich ochrony. Ocena ważności danych odbywałaby się na różnych poziomach administracyjnych państwa i byłaby także wynikiem zastosowania ustawowej definicji „danych istotnych" (ang. *important data*), nad którą również trwają prace legislacyjne. Chińskie prawodawstwo stara się jednak bilansować cele w zakresie bezpieczeństwa narodowego z wykorzystaniem danych do napędzania innowacji i gospodarki cyfrowej, dlatego zakłada ustanowienie rynków transakcji danymi (ang. *data transaction markets*). Dane określane są w nim jako piąty czynnik produkcji – po ziemi, pracy, kapitale i technologii – i aby zwiększyć ich użyteczność zakłada się, podobnie jak w UE, tworzenie branżowych baz danych. Projekt reguluje także m.in. aspekty związane z zagranicznym transferem danych, dostęp do danych w Chinach przez organy ścigania z innych krajów i sposób, w jaki transgraniczny przesył danych podlegałby kontroli eksportu w związku z typami danych mających znaczenie dla bezpieczeństwa narodowego[77].

3. Infrastruktura, hardware, software czyli wyścig technologiczny

Rywalizacja o dane odbywa się także w wyścigu technologicznym między mocarstwami, który może doprowadzic do rozerwania cyfrowych łańcuchów dostaw. Światowa konkurencja o dane odbywa się na wielu płaszczyznach technologicznych: internetowej infrastruktury do transmisji danych, czyli sieci internetowej i infrastruktury chmurowej, sprzętu komputerowego (hardware), platform i algorytmów „zasysających" dane, czyli w oprogramowaniu (software) oraz aplikacji mobilnych. Dane można zbierać na wszystkich tych poziomach, dlatego kraje konkurują obecnie w zakresie sieci 5G, przetwarzania w chmurze, sztucznej inteligencji, informatyki kwantowej. Wszystkie te technologie nie tylko zwiększają ilość generowanych danych, ale także radykalnie zmieniają sposoby ich przechowywania, przetwarzania, przesyłania, analizowania.

W tym kontekście znaczenia nabierają ostatnie decyzje rządu Indii i administracji USA nakładające w obu tych krajach restrykcje na rozpowszechnione chińskie aplikacje mobilne. Zakaz w konsekwencji odcinający obywateli Indii od 59 aplikacji mobilnych w czerwcu i kolejnych 47 w lipcu 2020 r. wydany został z obawy o bezpieczeństwo i prywatność danych użytkowników, w wyniku ich kradzieży poprzez aplikacje oraz przekazywania na serwery zlokalizowane poza Indiami. W uzasadnieniu wskazano, że kompilacja tych danych, ich eksploracja i tworzenie profili użytkowników przez podmioty wrogie i zagrażające bezpieczeństwu narodowemu i obronności Indii są głęboko niepokojące,

c Inaczej Rozporządzenie o Ochronie Danych Osobowych, RODO.

naruszają suwerenność i integralność kraju, a zatem wymagają podjęcia środków nadzwyczajnych[78]. Zakaz o podobnych konsekwencjach wprowadzony został w rozporządzeniach wykonawczych (ang. *executive orders*) wydanych przez Donalda Trumpa 6 sierpnia 2020 r. w odniesieniu do aplikacji TikTok i WeChat, a obowiązywać ma po 45 dniach od publikacji. Wskazano w nim, że obydwie aplikacje postrzegane są przez władze amerykańskie jako zagrożenie dla bezpieczeństwa narodowego i gospodarczego USA, gdyż ich producenci respektują żądania ze strony władz ChRL o udostępnianie danych obywateli, które są danymi osobowymi i zastrzeżonymi. Jednocześnie w uzasadnieniu tych decyzji podaje się, że pozyskiwane dane mogą być również „wykorzystywane do kampanii dezinformacyjnych przynoszących korzyści Komunistycznej Partii Chin"[79]. Prezydent Trump wpisał tę decyzję w całość działań odnoszących się do krajowego stanu zagrożenia w kwestii łańcucha dostaw obejmującego technologie i usługi ICT, który wprowadzony został zarządzeniem wykonawczym podpisanym przez niego 15 maja 2019 r.[80] Rozporządzenie, mimo że nie wymieniało Chin i chińskich firm z nazwy, ogłaszało jednak stan wyjątkowy w związku z zagrożeniami dla amerykańskiej infrastruktury komunikacyjnej i usług ze strony obcych krajów, a służyć miało rządowi do podejmowania decyzji wykluczających niektóre podmioty z amerykańskiego rynku.

Cyberbałkanizacja i rozrywanie łańcuchów dostaw odbywa się zatem także z udziałem firm technologicznych produkujących *hardware* i komponenty składające się na infrastrukturę, która musi być zgodna z krajowymi standardami. Obawy o dostęp do danych artykułowane są już od wielu lat przez władze USA w związku z budową sieci 5G. Narodowa Strategia Bezpieczeństwa 5G (ang. National Strategy to Secure 5G) opublikowana w marcu 2020 r. wskazuje na potrzebę budowy bezpiecznej i odpornej infrastruktury cyfrowej z uwagi na fakt, iż będzie ona atrakcyjnym celem dla przestępców i zagranicznych adwersarzy ze względu na dużą ilość danych, które przesyła i przetwarza, a także wsparcie, jakie 5G zapewni dla infrastruktury krytycznej. Strategia wskazuje, że przestępcy i zagraniczni adwersarze będą dążyć do kradzieży informacji przesyłanych przez te sieci w celu uzyskania korzyści finansowych oraz do wykorzystywania systemów i urządzeń podłączonych do sieci 5G dla gromadzenia danych wywiadowczych i inwigilacji[81]. Biorąc pod uwagę te zagrożenia, Amerykanie, ale także decydenci w wielu innych krajach, w tym w UE, zdają sobie sprawę, że infrastruktura 5G musi być bezpieczna i niezawodna, także po to, aby utrzymać bezpieczeństwo oraz prywatność danych i informacji, co jest podstawą bezpieczeństwa publicznego, narodowego i gospodarczego. Debata o dopuszczeniu chińskich firm do budowy sieci 5G w wielu krajach również koncentruje się wokół bezpieczeństwa i integralności danych, wskazując m.in. na legislacyjne uwarunkowania w ChRL. Chińskie narodowe prawo kontrwywiadowcze z 2014 r. (反间谍法), następnie doprecyzowane w 2017 r., wymaga bowiem od obywateli Chin, ale także organizacji, wspierania państwa w gromadzeniu informacji w każdym momencie, kiedy władze tego oczekują. Z kolei regulacje wdrażające te przepisy informują, że „gdy organy Bezpieczeństwa Państwa, które wykonują zadania kontrwywiadu zgodnie z prawem, zażądają od obywateli lub organizacji zapewnienia obiektów lub innej pomocy, są oni prawnie zobowiązani ją zapewnić"[82]. Przepisy te położyły się cieniem na dyskusję dotyczącą rozwoju sieci 5G przez Huawei, gdyż interpretowane są jako furtka do „zgodnego z chińskim prawem" instalowania backdoorów przez firmy technologiczne i budzą obawy zarówno o integralność danych, jak i o bezpieczeństwo sieci.

O kilka kroków dalej, jeśli chodzi o chęć utrzymania kontroli nad przepływem danych, idzie także inicjatywa amerykańskiego Departamentu Stanu ogłoszona 5 sierpnia 2020 r. przez szefującego temu ministerstwu Michaela Richarda Pompeo, nazwana „Czystą siecią" (ang. Clean Network). Plan zakłada kompleksowe podejście do „ochrony aktywów narodowych", w tym prywatności obywateli oraz najbardziej wrażliwych informacji firm przed Komunistyczną Partią Chin,

i ma stanowić odpowiedź na „długoterminowe zagrożenie dla prywatności danych, bezpieczeństwa, praw człowieka i współpracy opartej na zasadach"[83]. Działania proponowane przez USA mają w centrum uwagi **de facto dostęp do danych** i zakładają blokowanie amerykańskiego rynku przed dostawcami sprzętu i sieci telekomunikacyjnych, w tym 5G, aplikacjami mobilnymi (aby chronić najbardziej wrażliwe informacje osobiste i biznesowe Amerykanów na ich telefonach komórkowych), usługami w chmurze (aby chronić najbardziej wrażliwe prywatne informacje obywateli USA, własność intelektualną amerykańskich firm oraz wyniki badań, w tym nad szczepionkami na COVID-19), a także zapobiec gromadzeniu na „hiperskalę" przez ChRL danych, w tym wywiadowczych, przesyłanych za pośrednictwem podmorskich kabli telekomunikacyjnych. Jeśli dojdzie do realizacji tych założeń przez amerykańską administrację, możemy spodziewać się pogłębienia cyfrowego podziału świata, co w efekcie doprowadzić może nawet do rozerwania globalnego Internetu. W odpowiedzi na te plany chiński minister spraw zagranicznych Wang Yi przedstawił 7 września 2020 r. skierowaną również do społeczności międzynarodowej „globalną inicjatywę bezpieczeństwa danych" (ang. Global Initative on Data Security). Stawia ona w centrum uwagi dane i ich rolę w rozwoju gospodarki cyfrowej oraz realnej, przyspieszeniu przemian i budowie nowego rodzaju przemysłu. Pekin mówi wprost o ekonomicznym znaczeniu danych – wskazując, że „globalne dane stają się impulsem do rozwoju gospodarczego i odnowy przemysłowej każdego kraju. Jednocześnie zagrożenia bezpieczeństwa danych stanowią nowe wyzwania dla globalnego zarządzania cyfrowego"[84]. Inicjatywa to także wyzwanie rzucone USA i próba zmiany percepcji ChRL przez społeczność międzynarodową w zakresie podejścia Pekinu do tematu prywatności i integralności danych. W wystąpieniu minister Yi deklaruje bowiem, jakoby chińskie prawo zawierało jasne przepisy dotyczące ochrony praw i interesów obywateli i organizacji, w tym bezpieczeństwa danych i danych osobowych. Z kolei w wymiarze współpracy międzynarodowej podkreśla potrzebę wielostronnego dialogu na temat zarządzania Internetem, tworzenia zasad cyfrowej gospodarki i zarządzania danymi oraz niedopuszczania do upolitycznienia kwestii bezpieczeństwa danych. Jednocześnie przedstawia szereg postulatów, które są zmianą względem praktyk przypisywanych chińskim podmiotom, związanych chociażby z kradzieżą własności intelektualnej przedsiębiorstw czy atakami hakerskimi, postulując, aby technologie informatyczne nie były używane do kradzieży „istotnych danych"[85].

PODSUMOWANIE

Aktualna sytuacja geopolityczna pozwala wątpić, że temat zarządzania Internetem i danymi spotka się z chęcią konstruktywnej współpracy całej społeczności międzynarodowej. Spodziewać się zatem należy decyzji politycznych i regulacji w ramach poszczególnych krajów lub grup państw dzielących podobne cele geopolityczne. Państwa podobnie myślące powinny dążyć do porozumienia, kierując się wspólnymi wartościami oraz wyważyć interesy gospodarcze i polityczne. Zawiązująca się właśnie współpraca krajów Democracy10 w zakresie technologii 5G powinna być poszerzona nie tylko podmiotowo (o kraje UE i NATO), ale także przedmiotowo (obejmując cały cyfrowy łańcuch wartości). Prawdopodobnym scenariuszem, jeśli chodzi o rozrywanie łańcuchów dostaw (ang. *decoupling of supply chains*) i odwrócenie procesu globalizacji, wydaje się brak możliwości powrotu do poprzedniego stanu co najmniej w wymiarze technologicznym. Sektor technologiczny już zawsze będzie wymagał kontroli i międzynarodowych certyfikatów bezpieczeństwa[86]. Wyzwaniem cyberbezpieczeństwa będzie przede wszystkim zapewnienie, że dane pozostają bezpieczne w całym cyfrowym łańcuchu wartości. Wyzwaniem politycznym będzie natomiast pogłębiona i stała współpraca poprzez wywołanie co najmniej transatlantyckiej technologicznej *détente*[87] lub zawarcie, jak proponował Minister Marek Zagórski, transatlantyckiego sojuszu technologicznego[88]. Zaznaczyć tu należy, że z podobnym postulatem współpracy wyszły także Chiny,

zatem niewykluczone, że na naszych oczach budują się dwa bloki współpracy technologicznej, z dwiema grupami krajów grawitującymi ku dwu centrom. Lub też w przyszłości z trzema, jeśli UE postanowi pogłębiać działania zmierzające do suwerenności technologicznej i autonomii cyfrowej.

Aby zapobiec zwiększeniu zależności danego kraju w ramach światowej gospodarki opartej na danych, narodowe strategie powinny mieć na celu promowanie cyfrowej modernizacji i tworzenia wartości w ramach łańcuchów wartości danych cyfrowych (ang. *data value chains*), a także wzmocnienie krajowych zdolności w zakresie „udoskonalenia" zbiorów danych. Do tego konieczne będzie tworzenie odpowiednich polityk krajowych, aby lepiej wykorzystywać możliwości oraz radzić sobie z ryzykiem i wyzwaniami związanymi z ekspansją danych cyfrowych. ONZ zwraca uwagę, że regulacje dotyczące cyfrowych danych są skomplikowaną i złożoną kwestią, ponieważ dotykają „praw człowieka, handlu, ekonomii tworzenia i przechwytywania wartości, organów ścigania i bezpieczeństwa narodowego. Formułowanie polityk, które biorą pod uwagę i uwzględniają te różne wymiary jest trudne, niemniej jednak konieczne"[89]. Radę tę powinny sobie szczególnie wziąć do serca kraje rozwijające się, do grona których według rankingu Międzynarodowego Funduszu Walutowego należy wciąż pięć państw Trójmorza – Bułgaria, Chorwacja, Polska, Rumunia, Węgry[90]. Kraje Trójmorza powinny współpracować w tworzeniu reżimu danych, kooperacja ta powinna się także odbywać na poziomie UE, zwłaszcza że Bruksela podjęła próbę uregulowania tej materii w przedstawionej European Strategy for Data, ale także w Digital Services Act i EU Industrial Strategy. ONZ zwraca również uwagę, że wiele zmian w zakresie polityk może być bardziej efektywnych na poziomie regionalnym i międzynarodowym[91]. Kluczowe globalne pytania dotyczą przypisania własności i kontroli nad danymi, budowy zaufania konsumentów i ochrony prywatności danych, regulowania transgranicznych przepływów danych, polityki podatkowej[d] i prawa konkurencji oraz budowania odpowiednich umiejętności i możliwości wykorzystania danych cyfrowych do rozwoju i osiągnięcia skalowalnej innowacyjności[92]. Bardzo ważne wyzwanie dotyczy tego, jak zapewnić bardziej sprawiedliwy podział korzyści ekonomicznych z danych cyfrowych w wymiarze społecznym. W przebiegu współpracy, ale też rywalizacji o dane, kluczowym wyzwaniem wydaje się również zapewnienie bezpieczeństwa i prywatności danych. Kraje muszą w odpowiedni sposób rozwijać infrastrukturę ich przesyłu i gromadzenia (centra danych), które będą w stanie zarządzać przepływem ogromnych ilości informacji oraz zapewnić bezpieczeństwo używanych technologii ich przechowywania, w tym w modelu *storage at the edge*[e].

d Kwestia ta dyskutowana jest na poziomie Unii Europejskiej oraz OECD, celem tej ostatniej organizacji jest osiągnięcie konsensu do końca 2020 roku.

e Więcej na ten temat w następnym rozdziale.

PRZYPISY

1 Por. Nagy S. R., *Geotechnology meets geopolitics: US-China AI Rivalry and Implication for Trade and Security*, World Commerce Review, 2018.

2 Rosenbach E., Mansted K., *The Geopolitics of Information*, Harvard Kennedy School, 2019, s. 1.

3 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. xviii, [online:] https://unctad.org/en/PublicationsLibrary/der2019_en.pdf#page=19.

4 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. xix.

5 Harari Y., *Read Yuval Harari's blistering warning to Davos in full*, World Economic Forum, 22.07.2020, [online:] https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/.

6 „Detailed machine-readable information available about practically everything" – za: *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. 27.

7 Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa, 2020, s. 64.

8 Tamże, s. 67.

9 Tamże, s. 64, 65, 67.

10 Siegele L., *A deluge of data is giving rise to a new economy*, The Economist, 20.08.2020, [online:] https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy.

11 Tamże.

12 Tamże.

13 *Mobile Phone Market Forecast – 2019*, Areppim, 20.08.2020, [online:], https://stats.areppim.com/stats/stats_mobilex2019.htm.

14 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. 9.

15 Desjardins J., *How much data is generated each day?*, 10.07.2020, [online:] https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

16 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. 11.

17 Tamże, s. 12.

18 Tamże, s. 29.

19 Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020, s. 83.

20 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. 4.

21 Śledziewska K. , Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020, s. 79.

22 Rzemek M., *Otwarte dane publiczne napędzą nowe biznesy*, Rzeczpospolita, 28.08.2020, [online:] https://www.rp.pl/Urzednicy/308289959-Otwarte-dane-publiczne-napedza-nowe-biznesy.html.

23 Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa, 2020, s. 79.

24 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ , 2019, s. 29.

25 *A deluge of data is giving rise to a new economy*, 20.08.2020, [online:] https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy.

26 Tamże, s. 69.

27 Tamże, s. 70.

28 *Walmart enters race for TikTok US with Microsoft partnership*, Financial Times, 27.08.2020, [online:] https://www.ft.com/content/70551adb-7a6e-47a1-a6d1-070efaa957fd.

29 *Big Data = Big Challenges? Countering adversity in the data-driven economy*, Road to CYBERSEC, 20.08.2020, [online:] https://cybersecforum.eu/2020/08/03/big-data-big-challenges-countering-adversity-in-the-data-driven-economy/.

30 Tamże.

31 Tamże.

32 Tamże.

33 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. xix.

34 Tamże, s. xx.

35 Śledziewska K., Włoch R., *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa 2020, s. 84.

36 Tamże, s. 71.

37 Więcej: Albrycht I., Siudak R., Kanownik M., 危机 *[wēijī]*, Instytut Kościuszki, 20.08.2020, [online:] https://ik.org.pl/publikacje/%e5%8d%b1%e6%9c%ba-weiji-nowy-brief-programowy/.

38 Rosenbach E., Mansted K., *The Geopolitics of Information*, Harvard Kennedy School, 2019, s. 2.

39 Tamże, s. 1.

40 *Science & Technology Trends 2020-2040*, *Exploring the S&T Edge*, NATO Science & Technology Organization, 2020, s. 44.

41 Tamże.

42 Vinci A., *The Coming Revolution in Intelligence Affairs*, 05.09.2020, [online:] https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs.

43 *Geospatial Intelligence*, European Union Satellite Centre, 05.09.2020, [online:] https://www.satcen.europa.eu/page/geospatial_intelligence.

44 Vinci A., *The Coming Revolution in Intelligence Affairs*, 05.09.2020, [online:] https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs.

45 Tamże.

46 *Science & Technology Trends 2020-2040*, *Exploring the S&T Edge*, NATO Science & Technology Organization, 2020, s. 42.

47 Tamże, s. 45.

48 Stoltenberg J., *Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Industry Forum, Washington D.C.*, 20.08.2020, [online:] https://www.nato.int/cps/en/natohq/opinions_170786.htm.

49 *Science & Technology Trends 2020-2040*, *Exploring the S&T Edge*, NATO Science & Technology Organization, 2020, s. 45.

50 Scheid K. J., *What if NATO had no physical headquarters*, NITECH, nr 3, 2020, s. 12.

51 Tamże.

52 *Science & Technology Trends 2020-2040*, *Exploring the S&T Edge*, NATO Science & Technology Organization, 2020, s. 48.

53 Kim J., *Digital Twins and Data Analysis*, 20.08.2020, [online:] https://www.afcea.org/content/digital-twins-and-data-analysis.

54 *Cyberbalkanization and the Future of the Internets*, 20.08.2020, [online:] Medium, https://medium.com/skycoin/cyberbalkanization-and-the-future-of-the-internets-f03f2b590c39.

55 Kurbalija J., *The Internet and 'balkanisation through regulation'*, 20.08.2020, [online:] https://www.diplomacy.edu/blog/internet-and-%E2%80%98balkanisation-through-regulation%E2%80%99.

56 *Cyberbalkanization and the Future of the Internets*, 20.08.2020, [online:] Medium, https://medium.com/skycoin/cyberbalkanization-and-the-future-of-the-internets-f03f2b590c39.

57 Kapur A., *The Rising Threat of Digital Nationalism*, 20.08.2020, [online:] Wall Street Journal, https://www.wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577.

58 *Russia internet: Law introducing new controls comes into force*, BBC, 20.08.2020, [online:] https://www.bbc.com/news/world-europe-50259597.

59 Mayssa I., Keshav J., *Data localisation: From information protection to balkanisation of the Internet*, 20.08.2020, [online:] https://www.deltapartnersgroup.com/data-localisation-information-protection-balkanisation-internet.

60 Taylor C., *Government-led internet shutdowns cost the global economy $8 billion in 2019, research says*, CNBC, 20.08.2020, [online:] https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html.

61 Kapur A., *The Rising Threat of Digital Nationalism*, 20.08.2020, [online:] Wall Street Journal, https://www.wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577.

62 Albrycht I., *Białoruś – rewolucja on i offline*, Instytut Kościuszki, 20.08.2020, [online:] https://ik.org.pl/bialorus-rewolucja-on-i-offline-komentarz-izabeli-albrycht/.

63 *Data localization*, Wikipedia, 30.08.2020, [online:] https://en.wikipedia.org/wiki/Data_localization.

64 Mayssa I., Keshav J., *Data localisation: From information protection to balkanisation of the Internet*, 20.08.2020, [online:] https://www.deltapartnersgroup.com/data-localisation-information-protection-balkanisation-internet.

65 Tamże.

66 Tamże.

67 Boucher R., *Congress must act to stop balkanization of the internet*, Mercury News, 21.08.2020, [online:] https://www.mercurynews.com/2019/10/30/opinion-congress-must-act-to-stop-balkanization-of-the-internet/.

68 Gershkovich E., *The uneasy coexistence of Yandex and the Kremlin*, MIT Technology Review, 21.08.2020, [online:] https://www.technologyreview.com/2020/08/19/1006438/yandex-putin-arkady-volozh-kremlin/.

69 Roth A., *Russian internet giant grants veto powers to Kremlin-linked body*, The Guardian, 21.08.2020, [online:] https://www.theguardian.com/world/2019/nov/18/russian-internet-giant-yandex-grants-veto-powers-kremlin-linked-body.

70 Gershkovich E., *The uneasy coexistence of Yandex and the Kremlin*, 21.08.2020, [online:] https://www.technologyreview.com/2020/08/19/1006438/yandex-putin-arkady-volozh-kremlin/.

71 Maryssa I., Keshav J., *Data localisation: From information protection to balkanisation of the Internet*, 20.08.2020 [online:], https://www.deltapartnersgroup.com/data-localisation-information-protection-balkanisation-internet.

72 Balcewicz J., *Europejska strategia danych*, *NASK CyberPolicy* 20.08.2020, [online:] https://cyberpolicy.nask.pl/europejska-strategia-danych/.

73 *Angela Merkel urges EU to seize control of data from US tech titans*, Financial Times, 20.08.2020, [online:] https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca,.

74 Tamże.

75 Balcewicz J., *Europejska strategia danych*, *NASK CyberPolicy* 20.08.2020, [online:] https://cyberpolicy.nask.pl/europejska-strategia-danych/.

76 *Five Important Takeaways From China's Draft Data Security Law*, New America, 20.08.2020, [online:] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/.

77 Tamże.

78 *Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order*, Press Information Bureau, Government of India, 10.09.2020, [online:] https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206.

79 *Executive Order on Addressing the Threat Posed by WeChat*, 09.08.2020, [online:] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

80 *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, White House, 09.08.2020, [online:] https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

81 *National Strategy to Secure 5G*, White House, 10.09.2020, [online:] https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-committed-safeguarding-americas-vital-communications-networks-securing-5g-technology/.

82 Hoffman S., Kania E., *Huawei and the ambiguity of China's intelligence and counter-espionage laws*, The Strategist, 20.08.2020, [online:] https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.

83 Pompeo M., *The Clean Network*, US Department of State, 20.08.2020, [online:] https://www.state.gov/the-clean-network/.

84 *Translation: China Proposes 'Global Data Security Initiative'*, New Americe 10.09.2020, [online:] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/.

85 Tamże.

86 *China v America*, The Economist, 10.09.2020, [online:] https://www.economist.com/leaders/2020/07/18/china-v-america.

87 Foroohar R., *Europe and US can still compete with Chinese tech*, Financial Times, 10.09.2020, [online:] https://www.ft.com/content/cdd9322d-a0af-4bd8-b6ab-04d9fadcc301.

88 *CYBERSEC Washington Leaders' Foresight 2019 – Key Takeaways*, 10.09.2020, [online:] https://2019.cybersecforum.eu/en/washington/2019-takeaways/.

89 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. xx.

90 *World Economic and Financial Surveys*, International Monetary Fund, 05.09.2020, [online:] https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/groups.htm#oem.

91 *Digital Economy Report 2019*, *Value Creation and Capture: Implications for Developing Countries*, ONZ, 2019, s. xx.

92 Tamże, s. xix.

Dr Przemysław Roguski

GEOPOLITYKA CHMURY

WPROWADZENIE

W poprzednim rozdziale argumentowano, że dane są „nową ropą naftową" lub „tlenem" gospodarki cyfrowej. Podobna analogia może być zastosowana do chmury obliczeniowej (*cloud computing*). Tak jak wartość ropy naftowej zależy od specjalistycznej infrastruktury do jej wydobycia, rafinacji, magazynowania i transportu, wartość ekonomiczna danych zależy od infrastruktury informatycznej do ich przechowywania i przetwarzania. Mając to na uwadze, niniejszy rozdział poświęcony jest geopolityce chmury, omawiając przy tym kwestie kontroli nad jej infrastrukturą, jak również nad danymi przechowywanymi w ten sposób. Stwierdzi się w nim, że dostawcy usług w chmurze (*cloud service providers*, CSP) nie tylko dbają o jeden z fundamentów gospodarki cyfrowej, ale również odgrywają ważną rolę geopolityczną i są czynnikami strategicznej konkurencji między państwami.

CLOUD COMPUTING – KRÓTKI ZARYS

Chmurę obliczeniową najprościej zdefiniować jako „wszechobecny, dogodny dostęp sieciowy na żądanie do wspólnej puli konfigurowalnych zasobów obliczeniowych"[1], takich jak pamięć masowa, aplikacje i usługi. Składa się ona z trzech modeli usług: *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) i *Software as a Service* (SaaS), oferujących różne stopnie dostępu do infrastruktury i rozwiązań programowych w zależności od potrzeb klienta. Przechowywanie danych w chmurze i oferowanie usług w chmurze przynosi klientowi kilka korzyści. Przede wszystkim firmy nie muszą utrzymywać własnych serwerów i dużych działów technicznych, czuwających nad ich działaniem i chroniących je przed cyberatakami, ale mogą korzystać z zasobów, oprogramowania i wiedzy eksperckiej dostarczanych przez dostawców usług internetowych, którzy ze względu na

ekonomię skali mogą to robić w sposób konkurencyjny finansowo. Nic więc dziwnego, że *cloud computing* przyciągnął klientów zarówno z sektora prywatnego, jak i publicznego, w tym całe departamenty rządowe. Przetwarzanie w chmurze ma również duże zalety dla użytkowników, którzy mogą uzyskać dostęp do swoich danych i aplikacji na wybranym przez siebie urządzeniu za pośrednictwem Internetu.

Rynek chmury obliczeniowej został rozwinięty – i nadal jest zdominowany – przez trzy główne amerykańskie firmy technologiczne: Amazon (Amazon Web Services), Microsoft (Microsoft Azure) i Alphabet (Google Cloud Platform),[2] które łącznie posiadają 59% udziału w światowym rynku (szacowanym na 100 mld USD w 2019 roku), przy czym mniejsi amerykańscy operatorzy, tacy jak IBM i Oracle, dodają kolejne 8 procent[3]. Chińskie firmy również dynamicznie rozwijają swoją infrastrukturę chmury, a największymi graczami są firmy Alibaba i Tencent[4]. Rynek ten będzie nadal odnotowywał szybki wzrost: Unia Europejska szacuje, że w latach 2018–2025 globalna ilość danych wzrośnie pięciokrotnie, z 33 do 175 zettabajtów[5]. Jednocześnie z szacunków wynika, że nastąpi przejście od przetwarzania w chmurze do przetwarzania „na krawędzi sieci" (ang. *edge computing*), tj. rozproszonego przechowywania i przetwarzania danych na stale połączonych ze sobą inteligentnych urządzeniach lokalnych (ang. *smart connected objects*), w wyniku czego przetwarzanie 20% danych przejmą scentralizowane urządzenia informatyczne (centra danych), a 80% *smart objects* (w przeciwieństwie do 80% przez centra danych i 20% przez *smart objects* w 2018 r.)[6]. Niemniej jednak nawet w tym scenariuszu znaczenie chmury będzie nadal rosło.

Główną cechą charakterystyczną chmury obliczeniowej jest mobilność i możliwość przenoszenia danych. Dane nie muszą być już przechowywane lokalnie. Zamiast tego mogą znaleźć się w dużych parkach serwerowych obsługiwanych przez dostawców usług przechowywania danych w chmurze i firmy telekomunikacyjne, a dostęp do nich można uzyskać *ad hoc* z każdego miejsca na ziemi (pod warunkiem, że ma ono połączenie z Internetem) w przeglądarce internetowej lub dedykowanej aplikacji[7]. Dzięki temu dane w chmurze mają cztery wyjątkowe cechy, które będą istotne dla dalszej analizy:

- wysoka mobilność danych i łatwość ich przekazywania poza granice państwowe,
- podzielność i możliwość partycjonowania danych, co prowadzi do ich przechowywania na serwerach w wielu lokalizacjach,
- niezależność od lokalizacji, co prowadzi do łatwego dostępu zdalnego, oraz
- lokalizacja danych jest decyzją biznesową dostawcy usługi, chyba że państwa narzucają zasady lokalizacji danych[8].

CHMURY OBLICZENIOWE I GEOPOLITYKA

Chociaż dane są wysoce mobilne i niezależne od lokalizacji, rynek *cloud computing* nie jest wolny od istotnych geopolitycznych wpływów i skutków. Zarówno narodowość operatorów tych usług, jak i wybór lokalizacji centrów danych ma istotne konsekwencje geopolityczne. Pierwsza konsekwencja dotyczy innowacji technologicznych i okazji biznesowych. Posiadanie dostępu do technologii chmury i możliwości jej rozwoju daje państwom i przedsiębiorstwom większe szanse na szybszy rozwój ich gospodarek cyfrowych. Choć lokalizacja centrów danych jest decyzją biznesową dostawcy, zależy ona zazwyczaj od kilku kluczowych czynników, takich jak bliskość dużych punktów dostępu do Internetu, bliskość klientów i wykwalifikowanej siły roboczej, bezpieczeństwo, ceny energii, średnie roczne temperatury (ze względu na zapotrzebowanie na chłodzenie serwerów) oraz otoczenie prawne[9]. Nic więc dziwnego, że większość centrów danych znajduje się w dużych, połączonych międzynarodowo miastach w krajach rozwiniętych gospodarczo. Silna gospodarka napędza popyt na

moce obliczeniowe w chmurze, co z kolei napędza rozwój gospodarki cyfrowej i przyciąga przedsiębiorstwa nie tylko z państwa, w którym działa centrum danych, ale także z państw sąsiednich. W ten sposób omawiana technologia przyczynia się do przemiany niektórych lokalizacji w regionalne centra technologiczne i gospodarcze.

Drugą konsekwencją jest kontrola, jaką państwo może sprawować nad CSP. Dzieje się tak dlatego, że na mocy prawa międzynarodowego państwa posiadają jurysdykcję – tj. uprawnienie do ustanawiania i egzekwowania norm prawnych – nad osobami i przedmiotami znajdującymi się na ich terytorium[10]. **Oznacza to, że państwa mogą stosować swoje prawa zarówno do dostawców usług w chmurze działających na ich obszarze, jak i do danych znajdujących się na serwerach w ich granicach. Fakt ten daje państwom, na których terytorium znajdują się centra danych, wysoki stopień kontroli nad takimi danymi nie tylko własnych obywateli, ale również obywateli i podmiotów zagranicznych.** Ten stopień kontroli może być istotny dla realizacji zasadnych celów, takich jak na przykład egzekwowanie prawa, ale może również budzić obawy co do prywatności i bezpieczeństwa danych przekazywanych do obcych państw i tam przechowywanych. Obawy te są tym większe, gdy państwo nie tylko sprawuje kontrolę nad działalnością dostawców takich usług na swoim terytorium, ale również może ustanawiać i egzekwować przepisy, które mają wpływ na działalność CSP na całym świecie. Ma to miejsce szczególnie w przypadku, gdy najwięksi światowi dostawcy usług w chmurze, tacy jak Amazon, Microsoft i Google, mają swoje siedziby w jednym państwie.

SPRAWA *MICROSOFT IRELAND* I *CLOUD ACT*

Być może najlepszym przykładem stopnia kontroli państwa nad dostawcami usług w chmurze jest sprawa *Microsoft Ireland*. Sprawa ta rozpoczęła się w 2013 r., kiedy to federalni prokuratorzy w Południowym Dystrykcie Nowego Jorku uzyskali nakaz przeszukania i zajęcia informacji, w tym poczty elektronicznej, przechowywanych na koncie zarejestrowanym w serwisie e-mail firmy Microsoft w celu ujawnienia treści wiadomości osoby podejrzanej o handel narkotykami[11]. Microsoft przekazał prokuratorom metadane dotyczące komunikacji przechowywane na serwerach w Stanach Zjednoczonych, ale odmówił przekazania treści wiadomości przechowywanych na serwerach w Irlandii, argumentując, że rząd poszukiwał informacji za pomocą nakazu na mocy art. 2703 lit. a) ustawy o przechowywaniu informacji (Stored Communications Act)[12] i twierdząc, że sąd nie jest uprawniony do wydania nakazu przeszukania poza granicami USA[13]. Sędzia wydał jednak nakaz, orzekając, że nakaz na mocy art. 2703 lit. a) Stored Communications Act nie jest ekstraterrytorialny, ponieważ zgodnie z prawem Microsoft jest zobowiązany do przedstawienia wszystkich informacji znajdujących się w jego posiadaniu, niezależnie od ich przechowywania, a „przeszukanie" treści poczty elektronicznej miałoby miejsce w Stanach Zjednoczonych[14].

W odwołaniu amerykański Sąd Apelacyjny dla Drugiego Obwodu (tzn. obszaru stanów Connecticut, Nowy Jork i Vermont) uchylił postanowienie sądu pierwszej instancji[15]. Główną kwestią omawianą przez Sąd Apelacyjny było to, czy przepisy dotyczące nakazu przeszukania zezwalają na ich stosowanie ekstraterytorialne[16], co byłoby konieczne do obalenia tzw. „domniemania przeciwko ekstraterytorialności" (ang. *presumption against extraterritoriality*), które stanowi, że ustawa nie obejmuje zagranicy, chyba że Kongres wyraźnie tak postanowi[a]. Na podstawie wykładni językowej Stored Communications Act Sąd Apelacyjny doszedł do wniosku, że zdalne przeszukanie poczty elektronicznej przechowywanej na serwerze w Irlandii ma efekt ekstraterytorialny. W przeciwnym razie takie zdalne przeszukanie

a *Morrison v. National Australia Bank Ltd.*, US Supreme Court, 561 U.S. 247, 130 S.Ct. 2869, [online:] https://www.supremecourt.gov/opinions/09pdf/08-1191.pdf; analogiczne stanowisko niedawno w sprawie *RJR Nabisco, Inc. v. European Community*, US Supreme Court, 579 U.S. ___, 136 S.Ct. 2090, [online:] https://www.supremecourt.gov/opinions/15pdf/15-138_5866.pdf.

byłoby również możliwe, gdyby posiadacz konta był obywatelem irlandzkim, a ujawnienie informacji naruszałoby prawo irlandzkie. To z kolei stworzyłoby zagrożenie, iż wedle zasady wzajemności również obce rządy mogłyby bez zgody Stanów Zjednoczonych przeszukiwać dane przechowywane na serwerach w USA[17].

Ostatecznie sprawa trafiła do Sądu Najwyższego (US Supreme Court)[18], ale ten nie miał możliwości jej rozstrzygnięcia, ponieważ Kongres przyjął ustawę o wyjaśnianiu legalnego wykorzystania danych za granicą (Clarifying Lawful Overseas Use of Data Act, CLOUD Act) dwa tygodnie po ustnej rozprawie i zanim Sąd Najwyższy miał możliwość wydania decyzji[19]. Ustawa ta zmienia Stored Communications Act i wymaga od dostawców usług podlegających jurysdykcji USA przedstawienia danych na podstawie nakazu niezależnie od lokalizacji serwera, na którym są przechowywane[20]. Aby uwzględnić możliwość powstania sprzecznych zobowiązań prawnych na mocy prawa państwa, w którym dane są przechowywane, CLOUD Act ustanawia mechanizm umożliwiający dostawcom usług komunikacji elektronicznej zaskarżenie nakazu[21]. Jednakże warunki, na jakich nakaz ten może zostać zaskarżony, są dość restrykcyjne; aby go uchylić, dostawca musi wykazać, że klient, którego dane są poszukiwane, nie jest osobą przebywającą na terenie Stanów Zjednoczonych lub tam mieszkającą, oraz że przekazanie danych naruszyłoby prawo „uprzywilejowanego obcego rządu" (ang. *qualifying foreign government*)[22]. Ustawa przewiduje ponadto, że tylko rządy tych państw uznawane są za uprzywilejowane, z którymi Stany Zjednoczone zawarły umowę wykonawczą i których prawo przewiduje podobne uprawnienia na zasadzie wzajemności[23]. Ponadto ustawa ta znosi zakaz przekazywania danych obcym państwom, o ile takie państwa zaliczają się do grona państw uprzywilejowanych, a ich prawo krajowe zapewnia ochronę prywatności oraz respektuje powszechne prawa człowieka[24].

Konsekwencje ustawy CLOUD Act są zatem dwojakie. Po pierwsze, amerykańskie organy ścigania mogą zmusić amerykańskich dostawców omawianych usług do przedstawienia wszelkich danych w ich posiadaniu, niezależnie od narodowości „właściciela" danych lub lokalizacji, w są przechowywane. Po drugie, prawo amerykańskie reguluje, kiedy amerykańscy CSP mogą ujawnić stosownym służbom innych państw dane przechowywane na swoich serwerach, nawet jeśli dane te należą do obywateli lub firm tych państw. Należy jednak zauważyć, że konsekwencje te nie cechują wyłącznie CLOUD Act i Stanów Zjednoczonych, ale mogą pojawić się zawsze, gdy dane państwo posiada jurysdykcję nad dostawcami takich usług. Jest więc możliwe, a nawet prawdopodobne, iż Chiny mogłyby postąpić podobnie z danymi przechowywanymi w chmurze oferowanej przez firmy Tencent czy Alibaba.

EUROPEJSKA „SUWERENNOŚĆ CYFROWA"

Nietrudno zauważyć, że w opisanym powyżej systemie zaledwie kilka państw – tych, w których dostawcy usług w chmurze mają siedzibę lub prowadzą centra danych (tzw. państwa kontrolujące) – posiada wysoki poziom kontroli nad danymi. Pozostałym państwom pozostaje trudny wybór między zaakceptowaniem asymetrycznego stosunku sił i zależności od dobrej woli państw kontrolujących i ich gotowości do współpracy w zakresie dostępu do danych (biorąc pod uwagę, że tylko państwo kontrolujące może skutecznie egzekwować swoje zasady wobec dostawcy usług), albo odrzucenia obecnego modelu przetwarzania w chmurze i tym samym ryzyka odcięcia się od tej kluczowej technologii. Zależność od amerykańskich CSP i wynikająca z tego *de facto* ekstraterytorialność prawa amerykańskiego może być co prawda tolerowana przez wiele państw, ponieważ Stany Zjednoczone są demokratycznym państwem prawa, co zmniejsza ryzyko nadużycia władzy i czyni taką zależność przewidywalną. Ale nawet między bliskimi sojusznikami kontrola nad danymi stała się nie tylko kwestią biznesową, ale także czymś istotniejszym – kwestią suwerenności. Dowodem na to są ostatnie kroki Unii Europejskiej i niektórych jej państw członkowskich w kierunku stworzenia alternatywnego modelu chmury

obliczeniowej, który pomógłby odbudować europejską „suwerenność cyfrową".

Pojęcie „suwerenności cyfrowej" zostało po raz pierwszy rozwinięte we Francji (fr. *souveraineté numérique*)[25]. W 2019 roku francuski Senat powołał komisję badawczą ds. suwerenności cyfrowej w celu analizy tej kwestii i sformułowania zaleceń politycznych. Jej raport końcowy, przedstawiony przez sprawozdawcę Gérarda Longueta, krytycznie przeanalizował m.in. kwestię przechowywania danych w chmurze i jurysdykcji ekstraterytorialnej[26]. Stwierdzono w nim, że we współczesnym świecie dane stały się kwestią strategiczną z gospodarczego punktu widzenia (fr. *enjeu économique stratégique*), o ogromnym znaczeniu dla działalności głównych podmiotów gospodarki cyfrowej[27]. W sprawozdaniu omówiono obowiązek lokalizacji danych (trzymania danych na serwerach położonych na terytorium danego państwa) jako jeden ze sposobów ochrony danych, ale uznano go za rozwiązanie niedoskonałe[28]. Stwierdzono, że zasady lokalizacji danych mogą być ważne w odniesieniu do zabezpieczenia suwerenności cyfrowej w trzech przypadkach: gdy chodzi o dane „strategiczne" lub szczególnie wrażliwe, takie jak dane publiczne o znaczeniu dla suwerennych funkcji państwa, prywatne dane finansowe lub tajemnice handlowe, gdy zagwarantować należy dostęp do podstawowych usług oraz gdy trzeba wesprzeć przemysłowy ekosystem dostawców usług w chmurze[29]. W sprawozdaniu zwrócono jednak uwagę, że klauzule dotyczące lokalizacji danych nie zmniejszają ryzyka, które stwarzają zarówno przepisy ekstraterytorialne, takie jak ustawa CLOUD Act, jak i zależność niektórych przedsiębiorstw technologicznych od ich państw (jak w przypadku niektórych przedsiębiorstw chińskich)[30]. Raport skrytykował ponadto amerykańską ustawę jako zbyt szeroką w odniesieniu do objętych nią podmiotów, ujętych wykroczeń oraz rodzaju i ilości gromadzonych danych[31] i uznał ją za stwarzającą ryzyko nieautoryzowanego i niepożądanego dostępu amerykańskich organów ścigania do danych strategicznych osób prawnych (takich jak tajemnice handlowe), a także niezgodną z RODO w zakresie ochrony danych osobowych[32].

Aby ograniczyć to ryzyko, w sprawozdaniu zaleca się rozważenie trzech wariantów: po pierwsze, prawne oddzielenie spółek zależnych od spółek matek dla każdego regionu i lokalizacji geograficznej usług, tak aby amerykańskie organy ścigania nie miały dostępu do danych europejskich w oparciu o CLOUD Act; po drugie, zobligowanie przedsiębiorstw do sądowego kwestionowania nakazów wydania danych, które wydają się nieproporcjonalne lub bezzasadne; po trzecie, szerokie wykorzystanie solidnych technologii szyfrowania danych[33]. Raport Longueta, podobnie jak raport Raphaëla Gauvaina z 26 czerwca 2019 r.[34], zaleca wzmocnienie ustawy z 1968 r. o środkach blokujących, rozszerzenie ochrony RODO na nieosobowe dane firm oraz dążenie do szybkiego zawarcia umowy o współpracy między Unią Europejską a Stanami Zjednoczonymi[35].

Aczkolwiek żaden z tych środków nie został jeszcze wprowadzony w życie w momencie pisania niniejszego raportu, z raportów Gauvaina i Longueta wynika, że Francja jest głęboko zaniepokojona ekstraterytorialnym zasięgiem amerykańskich i chińskich organów państwowych, spowodowanym dominacją tych państw w sektorach *software* i *hardware*. Dlatego Paryż jest zdania, że musi podjąć zdecydowane działania – zarówno legislacyjne, jak i w zakresie polityki przemysłowej – aby chronić francuskie dane i francuskie interesy strategiczne przed zakusami państw obcych, nawet państw o podobnych poglądach, takich jak Stany Zjednoczone.

Podobne rozważania leżą u podstaw stanowiska Niemiec w odniesieniu do amerykańskich usług w chmurze. Od czasu afery Snowdena kraj ten jest głęboko zaniepokojony dostępem amerykańskiej Agencji Bezpieczeństwa Narodowego (National Security Agency, NSA) i organów ścigania USA do niemieckich danych. Rząd niemiecki wielokrotnie podkreślał, że choć uznaje, iż organy ścigania muszą otrzymać narzędzia konieczne do zwalczania cyberprzestępczości i stawić czoła wyzwaniom, jakie stwarza rozprzestrzenianie się transnarodowych usług w chmurze, każde przyjęte rozwiązanie

prawne musi respektować podstawowe gwarancje praw człowieka i umożliwiać współpracę między państwami na zasadzie równości. W tym celu rząd niemiecki opowiada się za szybkimi negocjacjami pomiędzy Komisją Europejską a rządem amerykańskim, aby zawrzeć umowę o współpracy w tym zakresie, jak przewiduje CLOUD Act[36]. Jednak oprócz zacieśniania współpracy międzynarodowej Niemcy dążą również do zabezpieczenia własnej „cyfrowej suwerenności" (niem. *digitale Souveränität*), ograniczając dostęp organów ścigania USA do niemieckich danych. Odbywa się to na dwa sposoby: po pierwsze, poprzez ograniczenie rodzaju danych, które mogą być przechowywane za pomocą amerykańskich dostawców chmury, a po drugie, poprzez opracowanie autonomicznego rozwiązania przechowywania danych w chmurze. W tym celu 29 października 2019 r. rząd niemiecki uruchomił projekt GAIA-X[b]. Uzasadnieniem dla tego projektu jest obrona europejskiej „suwerenności danych" (niem. *Datensouveränität*) przed rosnącym uzależnieniem od zagranicznych technologii cyfrowych[37]. W tym celu Niemcy chcą stworzyć infrastrukturę danych, która gwarantowałaby europejską kontrolę nad danymi obywateli Unii Europejskiej i zmniejszała zależność od zagranicznych dostawców usług w chmurze[38]. Ma to nastąpić przez połączenie infrastruktury scentralizowanej i zdecentralizowanej (*cloud computing* oraz *edge services*) w jeden spójny system, oparty na otwartych technologiach i zapewniający interfejsy ułatwiające wymianę danych i korzystanie z aplikacji[39]. Co najważniejsze, ma się to odbywać w oparciu o istniejące i dopiero budowane europejskie usługi i infrastrukturę oraz wyeliminować konieczność korzystania z usług amerykańskich dostawców, ograniczając w ten sposób narażenie danych na dostęp organów ścigania USA. Projekt GAIA-X został niedawno wsparty przez Komisję Europejską, która w *Europejskiej strategii w zakresie danych* zaproponowała rozwój wspólnej europejskiej przestrzeni danych oraz łączenie infrastruktur chmury obliczeniowej i umożliwienie dostępu do „konkurencyjnych, bezpiecznych i uczciwych" europejskich usług chmury obliczeniowej[40]. Pilną potrzebę poszukiwania europejskich rozwiązań w tej dziedzinie podkreśla orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Schrems II, w którym Trybunał orzekł, że prawo krajowe Stanów Zjednoczonych nie zapewnia ochrony danych osobowych Europejczyków, która byłaby zasadniczo równoważna z ochroną wymaganą przez prawo UE, i tym samym unieważnił Tarczę Prywatności UE–USA (zasady i zobowiązania ochrony danych dla amerykańskich firm z 2016 r.), uniemożliwiając przez to przekazywanie europejskich danych osobowych do USA[41].

ZAGROŻENIE ZE STRONY CHIN I INICJATYWA *CLEAN NETWORK*

Powyższe przykłady pokazują, że nawet sojusznicy mogą mieć zastrzeżenia do nadmiernej ekstraterytorialnej jurysdykcji przyjaznego mocarstwa i mogą chcieć rozwijać własne zdolności w tym zakresie. Zagrożenie jest znacznie większe, gdy infrastruktura chmury obliczeniowej i operatorzy tej infrastruktury znajdują się pod jurysdykcją mocarstwa nastawionego antagonistycznie, takiego jak Chiny. W tym przypadku obawy o bezpieczeństwo danych związane z zakresem kontroli państwa chińskiego nad chińskimi dostawcami chmury, takimi jak Tencent i Alibaba, oraz producentami sprzętu, takimi jak Huawei, w połączeniu z brakiem solidnej ochrony prawnej, a także licznymi przykładami nadużyć (takich jak kradzież własności intelektualnej), skłoniły Departament Stanu USA do ogłoszenia programu Clean Network[42]. Program ten ma na celu ochronę krytycznej amerykańskiej infrastruktury telekomunikacyjnej i technologicznej, a jego komponent Clean Cloud stanowi, że poufne dane osobowe oraz własność intelektualna nie powinny być „przechowywane i przetwarzane w systemach chmury dostępnych dla naszych zagranicznych przeciwników za pośrednictwem takich firm jak Alibaba, Baidu i Tencent".

b Raport o nim jest również dostępny po angielsku jako *Project GAIA-X. A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem*, Bundesministerium für Wirtschaft und Energie, 29.10.2019, [online:] https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.html.

CZY ISTNIEJE „TRZECIA DROGA"? PRZYKŁAD POLSKI

W poprzednich akapitach argumentowano, że chmura ma znaczące skutki geopolityczne ze względu na kontrolę nad danymi, którą państwo może sprawować, jeżeli dostawcy usług w chmurze posiadają siedzibę w danym państwie lub centra danych znajdują się na jego terytorium. Państwa mogą wybrać różne strategie radzenia sobie z wynikającą z tego asymetrią geopolitycznej siły: od pogodzenia się z istniejącą sytuacją i różnych stopni współpracy aż do kontestacji *status quo*, blokowania „nieprzyjaznych" platform i rozwijania własnych zdolności w tym zakresie.

Należy jednak zauważyć, że nie każde państwo europejskie podąża drogą do osiągnięcia „suwerenności cyfrowej" poprzez wyłączenie zagranicznych CSP z dostępu do kluczowych danych. W 2018 r. polski rząd uruchomił program Wspólna Infrastruktura Informatyczna Państwa, którego celem jest stworzenie dwóch usług tego typu: Publicznych Chmur Obliczeniowych oraz Rządowej Chmury Obliczeniowej[43]. Polskie władze nie wykluczają zagranicznych dostawców z polskiego rynku danych wrażliwych, a raczej stosują różne standardy bezpieczeństwa i dostępu do różnych rodzajów danych. Na przykład Publiczna Chmura Obliczeniowa (lub po prostu Chmura Krajowa) zostanie utworzona we współpracy z firmą Google, która zbuduje hub Google Cloud w Warszawie. Obecnie największym i strategicznym klientem Chmury Krajowej jest największy bank w Polsce, PKO BP, a oferta Chmury Krajowej jest skierowana głównie do sektora prywatnego. Z kolei administracja publiczna i samorządowa będzie mogła korzystać z Rządowej Chmury Obliczeniowej. Dla tej „chmury publicznej" rząd ustanowi wymogi bezpieczeństwa oraz Rządowy Klaster Bezpieczeństwa, najprawdopodobniej dla najbardziej wrażliwych danych[44]. Czy Polska dopuści zagranicznych dostawców chmury do rządowego klastra bezpieczeństwa i będzie próbowała zabezpieczyć dane państwowe (np. na podstawie zobowiązań kontraktowych lub szyfrowania danych), czy też całkowicie te podmioty wykluczy, nie jest jeszcze przesądzone. Należy jednak zauważyć, że Polska obecnie nie posiada alternatywy w postaci dużych krajowych dostawców takich usług i w związku z tym jest uzależniona od zewnętrznej wiedzy specjalistycznej w zakresie usług w chmurze, co ogranicza potencjalne dążenie do suwerenności cyfrowej.

Patrząc szerzej na Europę Środkową i Wschodnią (EŚW), dostrzec można dość podobną sytuację. Według autorów dwóch niedawnych raportów na temat rynku chmury w tym regionie[45] oczekuje się, że do 2022 r. w państwach EŚW będzie ponad 365 milionów użytkowników Internetu i ponad 2 miliardy podłączonych urządzeń. Jednocześnie tylko 13,1% badanych firm w regionie już dokonało cyfrowej transformacji (w tym korzysta z usług chmury obliczeniowej), a 76,4% firm dopiero stawia pierwsze kroki w tym kierunku. Oba te czynniki łącznie wskazują na dynamiczny rozwój rynku chmury w Europie Środkowo-Wschodniej oraz zwiększone zapotrzebowanie na inwestycje w odpowiednią infrastrukturę. Podobnie jak Polska, również inne kraje EŚW nie mają dużych krajowych operatorów świadczących usługi w zakresie przetwarzania danych, którzy mogliby sami udźwignąć te inwestycje, i będą musiały zdecydować, jak rozwijać swoje rynki, aby jak najlepiej służyły potrzebom zarówno sektora publicznego, jak i prywatnego. Również w tym przypadku wybór będzie podyktowany zarówno względami geopolitycznymi, jak i biznesowymi.

WNIOSKI

W artykule argumentowano, że chmura obliczeniowa nie powinna być postrzegana wyłącznie z perspektywy biznesowej. Raczej, ze względu na znaczenie danych dla nowoczesnej gospodarki cyfrowej i bezpieczeństwa narodowego, możliwości przechowywania i przetwarzania danych w chmurze zyskały szczególne znaczenie dla technologicznej lub cyfrowej suwerenności państwa, a tym samym stanowią ważny czynnik w obecnej geoekonomii i geopolityce. Ostatnie

przykłady, takie jak amerykańska ustawa CLOUD Act, europejskie próby rozwoju własnych platform chmury oraz amerykańskie inicjatywy na rzecz ochrony wrażliwych danych prywatnych i biznesowych przed dostępem państwa chińskiego, są tego dowodem. W tej wrogiej rzeczywistości geopolitycznej Europa Środkowa musi wybrać, którą drogą podążać. Ze względu na wyznawane wartości, takie jak praworządność i ochrona praw podstawowych, oraz strukturę sojuszy wydaje się oczywiste, że państwa Trójmorza nie mogą popaść w technologiczną zależność od Chin. Powinny raczej dążyć do rozwijania własnych zdolności w tym obszarze we współpracy z sojusznikami amerykańskimi i europejskimi. Projekty polskiej Chmury Krajowej i Rządowej Chmury Obliczeniowej są krokiem w tym kierunku i dlatego mogą być wzorem do naśladowania dla całego regionu.

PRZYPISY

1 Mell P., Grance T., *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Special Publication 800-145, 2011, s. 2 („ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources").

2 Dignan L., *Top cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players*, ZDNet, 11.05.2020, [online:] https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/.

3 Richter F., *Amazon leads $100 Billion Cloud Market*, Statista, 11.02.2020, [online:] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

4 *Tamże*.

5 *Europejska strategia w zakresie danych*, Unia Europejska, 02.2020, s. 2, https://ec.europa.eu/commission/presscorner/api/files/attachment/862132/European_data_strategy_pl.pdf.pdf.

6 *Tamże*.

7 *Wniosek. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych*, Komisja Europejska, 17.04.2018, Doc. COM(2018) 225, s. 16, [online:] eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018PC0225.

8 Daskal J., *The Un-Territoriality of Data*, „Yale Law Journal", Vol. 125, No 2, 2015, s. 365–377.

9 Burrington I., *The Strange Geopolitics of the International Cloud*, „The Atlantic", 17.11.2015, [online:] https://www.theatlantic.com/technology/archive/2015/11/the-strange-geopolitics-of-the-international-cloud/416370/.

10 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174 United Nations General Assembly, [online:] https://undocs.org/A/70/174.

11 *In Re Warrant to Search a Certain E-Mail Account*, US District Court (S.D. New York), 15 F.Supp.3d 466 (2014), 468, [online:] https://cite.case.law/f-supp-3d/15/466/.

12 *Stored Communications Act*, United States Congress, 18 U.S.C., § 2701-2712, [online:] https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim.

13 *In Re Warrant to Search a Certain E-Mail Account*, US District Court (S.D. New York), 25.04.2014, 15 F.Supp.3d 466 (2014), 470, [online:] https://cite.case.law/f-supp-3d/15/466/.

14 *Tamże*, s. 471–472; sąd stwierdził też, że „nakaz wydany na mocy tej ustawy […] nie wiąże się z wysłaniem przedstawicieli organów ścigania za granicę, nie wymaga nawet fizycznej obecności pracowników dostawcy usług w miejscu przechowywania danych […]. Nakłada jedynie na dostawcę usług obowiązek działania na obszarze Stanów Zjednoczonych" – *Tamże*, s. 475–476.

15 *Microsoft Corp. v. USA (In Re Search Warrant)*, US Court of Appeals for the Second Circuit, 829 F.3d 197 (2016), [online:] https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html.

16 *Tamże*, s. 210.

17 *Tamże*, s. 58–59.

18 *United States v. Microsoft Corp*., US Supreme Court, Docket No. 17-2, [online:] https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/.

19 *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, as part of the Consolidated Appropriations Act, United States Congress, 2018, Pub. L. 115-141, amending the Stored Communications Act, 18 U. S. C. §2701 i nast., [online:] https://www.govinfo.gov/content/pkg/PLAW-115publ141/html/PLAW-115publ141.htm.

20 Galbraith J., *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, „American Journal of International Law", 2018, Vol. 112, No 3, s. 486–487.

21 *Tamże*., s. 489.

22 *CLOUD Act*, 18 U.S.C. §2703(2)(A).

23 *Tamże*., §2703(1)(A).

24 Galbraith J., *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act…*, op. cit., s. 491.

25 Zob. Bellanger P., *La souveraineté numérique*, Stock, 2014; Türk P., Vallar Ch. (red.), *La souveraineté numérique : le concept, les enjeux*, Mare & Martin, 2018.

26 Longuet G., *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique*, French Senate – Commission d'enquête sur la souveraineté numérique, 1.10.2019, [online:] http://www.senat.fr/rap/r19-007-1/r19-007-1.html („Raport Longueta").

27 Raport Longueta, op.cit., s. 54.

28 *Tamże*, s. 68.

29 *Tamże*.

30 *Tamże*, s. 69.

31 *Tamże*, s. 71.

32 *Tamże*, s. 72.

33 *Tamże*, s. 74.

34 Gauvain M., *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, Francuskie Zgromadzenie Narodowe, 26.06.2019, [online:] https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf.

35 Raport Longueta, op.cit., s. 75.

36 Zob. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE*, Deutscher Bundestag, 11.07.2018, BT-Drs. 19/3392, s. 2, [online:] https://dip21.bundestag.de/dip21/btd/19/033/1903392.pdf.

37 *Tamże*, s. 6.

38 *Tamże*, s. 9.

39 *Tamże*, s. 12.

40 *Europejska strategia w zakresie danych*, Komisja Europejska, 19.02.2020, COM(2020) 66 final, [online:] eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0066.

41 *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*, Trybunał Sprawiedliwości Unii Europejskiej, sprawa C-311/18, wyrok z dn. 16.07.2020, [online:] http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=17518176.

42 *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, U.S. Department of State, 5.08.2020, [online:] https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.

43 *Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"*, Rada Ministrów, 24.09.2019, Monitor Polski 2019 r. poz. 862, [online:] https://monitorpolski.gov.pl/MP/2019/862.

44 *Tamże*.

45 Kroa V., Zajonc P., *Central and Eastern Europe Cloud Services Market: 2019–2023 Forecast and 2018 Vendor Shares*, International Data Corporation, 2019, [online:] https://services.idc.com/research/viewtoc.jsp?containerId=EUR244725719; *Central and Eastern European Data Center Markets – Investment Analysis and Growth Opportunities 2020-2025*, ResearchAndMarkets.com, 2020, [online:] https://www.researchandmarkets.com/reports/5067353/central-and-eastern-europe-data-center-market.

Paweł Kostkiewicz, Maciej Siciarek,
Krzysztof Silicki, Dr Magdalena Wrzosek
NASK PIB

CERTYFIKACJA I STANDARYZACJA W KONTEKŚCIE CYFROWEJ SUWERENNOŚCI

Na początku 2020 roku[a] Komisja Europejska ogłosiła nową Europejską strategię transformacji cyfrowej UE (ang. Shaping Europe's digital future). Silny nacisk położony został na cyfrową suwerenność w kontekście zapewnienia integralności i odporności sieci teleinformatycznych. Zdaniem KE wymaga to stworzenia odpowiednich warunków, umożliwiających rozwój i wdrożenie własnych zdolności w tym zakresie tak, aby Europa mogła się uniezależnić od technologii tworzonej w innych częściach świata[1]. Elementem tych działań jest tworzenie zrębów europejskiej certyfikacji produktów i usług ICT, wprowadzone przez Akt o Cyberbezpieczeństwie[2].

O ile w pierwszych dyskusjach nad cyfrową suwerennością jedną z istotniejszych kwestii było bezpieczeństwo danych, o tyle obecnie są to przede wszystkim aspekty technologiczne: normalizacja i certyfikacja produktów i usług, której szczególnym przykładem jest europejskie podejście do wprowadzenia sieci mobilnej nowej generacji (5G) oraz kwestie związane z bezpieczeństwem łańcucha dostaw.

Proces standaryzacji odnosi się do tworzenia specyfikacji wymagań (standardów), natomiast sama certyfikacja to proces wydawania dokumentów potwierdzających spełnienie wymagań określonych

a Komisja Europejska opublikowała komunikat *Shaping Europe's digital future* 19 lutego 2020 roku.

w standardach. O ile ani standaryzacja, ani certyfikacja ICT nie są niczym nowym, o tyle trwające obecnie globalne procesy związane z cyfrową rewolucją sprawiają, że kwestie te nabierają coraz większego znaczenia i stają się przedmiotem rywalizacji pomiędzy poszczególnymi państwami. Wyznaczanie standardów w szybko rozwijających się dziedzinach, takich jak cyberbezpieczeństwo i ICT, to pewnego rodzaju wyścig z czasem, toczący się w cieniu sprzecznych interesów. Jednostki odpowiedzialne za wyznaczanie standardów oraz instytucje państwowe odpowiedzialne za bezpieczeństwo kładą duży nacisk na sprawdzone i zweryfikowane rozwiązania technologiczne, których stosowanie gwarantuje pewien poziom cyberbezpieczeństwa. Natomiast konsumenci i producenci rozwiązań, którym zależy na przewadze konkurencyjnej, wywierają nacisk związany z jak najszybszym wprowadzaniem coraz bardziej złożonych technologicznie rozwiązań na rynek, co nie zawsze sprzyja trosce o odpowiedni poziom bezpieczeństwa. Dodatkowo, same standardy są w pewien sposób statyczne – stanowią obraz konkretnej sytuacji w konkretnym czasie – co stoi w wyraźnej opozycji do potrzeb rynku ICT, który jest niezwykle dynamiczny i cały czas się rozwija. Działania UE w tym zakresie są w rzeczywistości próbą ochrony rynku wewnętrznego Unii przed niesprawdzonymi produktami i rozwiązaniami z zewnątrz. W realiach trwającej amerykańsko-chińskiej rywalizacji technologicznej, Europa koncentruje się przede wszystkim na tym, aby rewolucja cyfrowa przebiegała w sposób jak najbezpieczniejszy. Ma to sprzyjać rozwojowi Jednolitego Rynku Cyfrowego[b], dzięki czemu możliwy będzie wzrost siły gospodarczej państw europejskich.

SUWERENNOŚĆ CYFROWA – ZARYS PROBLEMU

Pojęcia „suwerenność" użył po raz pierwszy francuski prawnik i teoretyk państwa Jean Bodin[c], według którego jest to absolutna, trwała, wieczna i niepodzielna władza nad ludźmi, która spaja państwo i pozwala na zachowanie niezależności wewnętrznej i zewnętrznej. Koncepcja ta jest często określana „władzą skutecznie działającą". W stosunkach międzynarodowych prawna definicja suwerenności została po raz pierwszy użyta w 1928 roku w sprawie *Island of Palmas*[d]. Definicja ta zakłada, że: „suwerenność w relacji pomiędzy państwami oznacza niezależność. Polega ona na egzekwowaniu funkcji państwa, niezależnie od części świata, w której znajduje się dane terytorium"[3]. Natomiast pojęcia „cyfrowa suwerenność" po raz pierwszy użył Pierre Bellanger[e], kiedy w 2011 roku opisał ją jako „kontrolę nad naszą teraźniejszością i przyszłością związaną z wykorzystaniem technologii i sieci komputerowych"[4].

Na poziomie Unii Europejskiej dyskusja na temat cyfrowej suwerenności trwa już od dłuższego czasu. W związku z budową w Europie tzw. Jednolitego Rynku Cyfrowego, wielokrotnie powracał temat wzrastającej dominacji ekonomicznej i politycznej GAFA, czyli największych technologicznych gigantów (Google, Apple, Facebook, Amazon). Uwagę zwracano m.in. na algorytmy kontrolujące dostęp do wiedzy, prowadzenie kampanii wyborczych w mediach społecznościowych, a także na kontrolę nad danymi użytkowników sieci. Wskazywano przy tym, że wiedza GAFA o internautach jest niejednokrotnie większa niż wiedza poszczególnych państw o ich własnych

b 6 maja 2015 roku Komisja Europejska przyjęła Strategię Jednolitego Rynku Cyfrowego dla Europy (A Digital Single Market Strategy for Europe). Głównym założeniem jest stopniowe usuwanie barier pomiędzy państwami członkowskimi na rynku cyfrowym. Według analiz KE, przyniesie to unijnej gospodarce 415 mld euro rocznie, co spowoduje znaczny wzrost gospodarczy w UE oraz powstanie nowych miejsc pracy. Strategia ta, wraz z uzupełniającymi ją regulacjami prawnymi umożliwia państwom członkowskim jak najpełniejsze wykorzystanie rewolucji cyfrowej i szybki wzrost gospodarczy.

c *Sześć ksiąg o Rzeczypospolitej* Bodina stało się podstawą francuskiej monarchii absolutnej, wprowadzonej za panowania Ludwika XIV.

d *Island of Palmas case* dotyczyła sporu pomiędzy USA a Holandią na temat przynależności wysp do tych państw. Stały Trybunał Arbitrażowy przyznał rację argumentacji Holandii.

e Założyciel i CEO francuskiej stacji radiowej Skyrock oraz sieci społecznościowej skyrock.com.

obywatelach. Elementy tej dyskusji wybrzmiewały także przy okazji negocjacji Dyrektywy NIS[5], kiedy podkreślano konieczność objęcia szczególnym nadzorem kluczowych sektorów gospodarki, takich jak energetyka, finanse czy transport. Komplementarnym działaniem są regulacje sektorowe w zakresie telekomunikacji. Dopiero od niedawna jednak wszystkie te elementy są przez decydentów postrzegane kompleksowo, właśnie w kontekście cyfrowej suwerenności. Także samo pojęcie używane jest od niedawna – UE zaczęła je stosować dopiero pod koniec 2018 roku. Polityka UE wpisuje się w szeroką międzynarodową dyskusję na temat cyfrowej suwerenności i obowiązywanie prawa międzynarodowego w cyberprzestrzeni[f].

Tallinn Manual 2.0[g] definiuje pięć zasad cyfrowej suwerenności[6]:

1. Zasada suwerenności państwa obowiązuje w cyberprzestrzeni.
2. Suwerenność wewnętrzna w cyberprzestrzeni jest związana z infrastrukturą teleinformatyczną, osobami oraz aktywnością mającą miejsce na terytorium państwa, z zastrzeżeniem międzynarodowych zobowiązań prawnych.
3. Suwerenność zewnętrzna w cyberprzestrzeni jest związana z wolnością do podejmowania działań w cyberprzestrzeni w relacjach międzynarodowych, z zastrzeżeniem międzynarodowych zobowiązań prawnych.
4. Naruszenie suwerenności w cyberprzestrzeni odnosi się do zakazu podejmowania operacji w cyberprzestrzeni naruszających suwerenność innego państwa.
5. Immunitet suwerenności i nienaruszalności oznacza, że jakakolwiek ingerencja państwa w infrastrukturę teleinformatyczną należącą do innego państwa, niezależnie od tego, gdzie się znajduje, stanowi naruszenie suwerenności.

Na podstawie tych zasad państwo ma m.in. prawo odłączenia od sieci każdej infrastruktury teleinformatycznej, która znajduje się na jego terytorium i której działanie może stanowić naruszenie suwerenności państwa[7]. Dodatkowo suwerenność wewnętrzna oznacza, że państwo może, częściowo lub w całości, ograniczyć dostęp do sieci osobom znajdującym się na jego terytorium, w szczególności do określonych treści online[8]. Istnieje także zasada powstrzymywania się od wrogich działań w cyberprzestrzeni[9]. Suwerenność zewnętrzna oznacza natomiast, że państwa mogą angażować się w działalność w cyberprzestrzeni w stosunkach międzynarodowych, zgodnie z własnymi decyzjami, o ile nie naruszają norm prawa międzynarodowego[10]. Naruszeniem suwerenności jest każda ingerencja w granicach terytorium państwa związana z działaniami w cyberprzestrzeni. Jako przykład eksperci podają użycie przez dane państwo nośnika USB ze złośliwym oprogramowaniem, żeby zakłócić działalność systemów na terytorium innego państwa[11]. W tym celu konieczne jest jednak dokonanie atrybucji, a więc przedstawienie dowodów, że za działanie to odpowiada inne państwo.

f Od 2003 roku przy ONZ działa GGE (Grupa ekspertów rządowych ds. rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego), której kolejne „edycje" analizują kwestie zastosowania prawa międzynarodowego w cyberprzestrzeni. Największe osiągnięcia miała trzecia grupa GGE, obradująca w latach 2012–2013, która uznała, że prawo międzynarodowe ma zastosowanie w cyberprzestrzeni. Grupa zgodziła się, że działalność państw w Internecie, również działalność infrastruktury informacyjno-komunikacyjnej na terytorium danego państwa, podlega Karcie Narodów Zjednoczonych, normom i zobowiązaniom dotyczącym suwerenności państwowej oraz pozostałym przepisom prawa. Po tych ustaleniach w pracach grupy doszło niestety do impasu. Obrady grupy piątej zakończyły się brakiem konsensusu, a obecnie nad wyzwaniami pracuje grupa szósta, która ma przedstawić swój raport pod koniec 2021 roku.

g Wydawnictwo jest owocem prac międzynarodowej grupy ekspertów, powołanej przy Cooperative Cyber Defence Centre of Excellence w Tallinie, która pracowała w latach 2009–2012. Grupa prowadzona była przez prof. Michaela N. Schmitta, przewodniczącego departamentu prawa międzynarodowego w United States Naval War College.

NORMALIZACJA, STANDARYZACJA I CYBERBEZPIECZEŃSTWO

Przejawem cyfrowej suwerenności jest normalizacja i certyfikacja produktów oraz usług ICT. Pojęcia te często stosowane są zamiennie. Tymczasem istnieje zasadnicza różnica pomiędzy normą a standardem. Warto także podkreślić, że działania w tym zakresie prowadzone są od dawna na wielu forach międzynarodowych, jednak dzięki wprowadzeniu w 2019 roku Aktu o Cyberbezpieczeństwie[12] w Europie rozpoczyna się nowy rozdział – **certyfikacja cyberbezpieczeństwa** – silnie powiązany z zagadnieniem cyfrowej suwerenności i próbą zagwarantowania przez państwa europejskie odpowiedniego poziomu bezpieczeństwa dla nowych technologii i usług.

Zgodnie z definicją Polskiego Komitetu Normalizującego norma (ang. standard) to „dokument przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie"[13]. **Zarówno w Polsce, jak i w Europie normalizacja nie jest obowiązkowa. Co oznacza, że zarówno tworzenie norm, jak i ich stosowanie jest dobrowolne[14]. Trochę inaczej jest w USA, gdzie standardy w zakresie ICT opracowuje NIST (*National Institute of Standards and Technology*). Opracowane przez nich standardy stają się obowiązujące, ale równocześnie na rynku amerykańskim funkcjonują także normy międzynarodowe, których stonowanie jest dobrowolne.**

Jednostką organizacyjną upoważnioną do wydawania norm w Polsce jest Polski Komitet Normalizacyjny (PKN). W odniesieniu do jednostek normalizacyjnych używane są także pojęcia SDO (*standards developing organization*), SSO (*standards setting organization*) i ESOs (*European Standards Organizations*). Dla konsumentów i producentów w Europie szczególnie istotne są przede wszystkim europejskie organizacje regionalne: Europejski Komitet Normalizacyjny (CEN), Europejski Komitet Normalizacyjny Elektrotechniki (CENELEC) i Europejski Instytut Norm Telekomunikacyjnych (ETSI). To właśnie one, jako organizacje stanowiące (publikujące) normy europejskie[15], odgrywają szczególną rolę na wspólnotowym rynku wewnętrznym. Ponieważ mamy do czynienia z wciąż postępującą konwergencją światów telekomunikacji, informatyki i elektrotechniki, przy publikacji nowych norm zacieśnia się współpraca wszystkich trzech instytucji. Dobrym przykładem jest współpraca ETSI TC CYBER z CEN/CENELEC JTC 13. ETSI TC CYBER, w ramach tzw. *Technical Committee* (TC), zajmuje się tematami związanymi z cyberbezpieczeństwem[h]. Dodatkowo centrum eksperckie dostarcza także rozwiązań w zakresie standaryzacji/normalizacji bezpieczeństwa IT, porad i wskazówek dla użytkowników, producentów, operatorów sieci oraz infrastruktury czy usług, a także dla regulatorów. W przeciągu ostatniego roku w ETSI, w ramach komitetu technicznego CYBER, prowadzono prace nie tylko nad bardzo aktualnymi obszarami technologicznymi np. tematyką Internetu rzeczy (nowa norma ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements*), ale również bardzo ciekawym zagadnieniem zabezpieczania cyfrowego materiału dowodowego na potrzeby postępowań sądowych[16].

Dodatkowo europejskie organizacje normalizacyjne mają swoje globalne odpowiedniki: ISO (the International Organization for Standardization), IEC (the International Electrotechnical Commission) and ITU-T (the International Telecommunication Union – Telecommunication Standardization Sector). Poza tym na wszystkich kontynentach funkcjonują także regionalne organizacje normalizacyjne, a wypracowane przez nie dokumenty mogą być dla przedsiębiorcy operującego globalnie równie ważne, jak polskie czy europejskie normy. **Normalizacja przekłada się bezpośrednio i pośrednio na oferowane produkty IT, może istotnie wpłynąć na dobór technologii czy technik**

h Prace w zakresie komitetu technicznego CYBER.

wytwarzania. Przyczyną tego oddziaływania jest presja rynku, który zgodność z normami traktuje jak wyznacznik jakości oraz metodę weryfikacji, czy produkt zostanie skutecznie wprowadzony do sprzedaży i użycia. I tutaj pojawia się zagadnienie oceny zgodności.

Certyfikacja to zwieńczenie oceny zgodności, jak również element kontroli i nadzoru rynku. **Certyfikat oznacza potwierdzenie, że wyrób, czasem sam projekt wyrobu lub proces jego wytwarzania, są zgodne z konkretnymi wymaganiami. Bardzo częstą praktyką jest weryfikacja zgodności z wymaganiami ustanowionymi przez normy.** Logika działania jest więc następująca: najpierw powstaje specyfikacja, która w wyniku konsensu staje się normą, a na jej podstawie dokonuje się oceny zgodności i w efekcie certyfikacji. Dlatego tak ważne jest to, co znajduje się w dokumentach normalizacyjnych i tak istotny jest udział w pracach normalizacyjnych, zarówno dla państwa, jak dla grup konsumenckich i organizacji przedsiębiorców[i]. Powołanie na normy w przepisach często zostaje wprost przeniesione do procesów zakupowych. Jako że zgodność z przepisami jest obligatoryjna, to najprostszym sposobem dowodzenia zgodności z regulacją jest przedłożenie dowodu spełnienia warunków, co w praktyce oznacza posiadanie certyfikatu. W związku z tym **w ostatnim czasie zagadnienia związane z normalizacją, oceną zgodności i certyfikacji znalazły się w oficjalnym dyskursie geopolitycznym, w związku z coraz większym naciskiem na kwestię cyfrowej suwerenności[j].**

Ważnym elementem cyfrowej suwerenności jest organizacyjna i operacyjna zdolność do certyfikacji wyrobów, systemów czy osób. W obszarze cyberbezpieczeństwa istnieje ugruntowana pozycja certyfikacji produktów IT w oparciu o normę potocznie nazywaną *Common Criteria* (dostępna jako PN-ISO/IEC 15408). Dzięki podpisanym przez NASK międzynarodowym porozumieniom SOG-IS[17] (Europa) i CCRA[18] (świat). Polska należy do grupy państw rozpoznających certyfikaty produktów w oparciu o tę normę[k]. W Polsce rozpoznaje się certyfikaty wystawiane przez jednostki certyfikujące z krajów posiadających takie możliwości. Już niedługo, dzięki realizowanemu w konsorcjum trzech instytutów badawczych projektowi badawczo-rozwojowemu[l], Polska dołączy do grona państw dysponujących takim potencjałem. W ramach tego konsorcjum powstały w Polsce jednostka certyfikująca (NASK) i dwa laboratoria specjalistyczne (IŁ, EMAG) do badania produktów IT pod kątem zgodności z normą *Common Criteria*. Obecnie trwają pierwsze pilotażowe projekty certyfikacji zgłoszone przez polskich producentów.

W obszarze certyfikacji systemów, a w szczególności systemu zarządzania bezpieczeństwem informacji, zarówno w Polsce, jak i Europie jest już długoletnie doświadczenie. Natomiast potencjał oceny i certyfikacji w zupełności wystarcza na potrzeby rynku. Dobrą podstawę legislacyjną stworzyły Krajowe Ramy Interoperacyjności[19], a następnie Ustawa o krajowym systemie

i Praca w Komitetach jest dobrowolna, a udział w pracach Komitetu może zgłosić każdy przedsiębiorca. Podobnie otwarty jest udział w pracach ESO, w szczególności warto pomyśleć o udziale w wybranej Industry Specification Group (ISG) – grup działających pod auspicjami ETSI, które pracują nad tematami od 5G po sztuczną inteligencję (SI).

j Jako państwo i szerzej kraj członkowski Unii Europejskiej mamy wpływ na stanowienie krajowych i europejskich przepisów. Znaną i dobrą praktyką legislacyjną jest powoływanie się na normy poprzez powołanie (odesłanie). W obszarze cyberbezpieczeństwa widać tego przykłady np. prace normalizacyjne ETSI wspierają dyrektywę EIDAS, krajowa inicjatywa „Wspólna Infrastruktura Informatyczna Państwa" powołuje normy PN-EN ISO/IEC 27001, PN-EN ISO 22301, PN-ISO/IEC 27005, PN-EN 50600.

k Obie umowy w oparciu o pełnomocnictwo Ministra Cyfryzacji podpisał NASK Państwowy Instytut Badawczy, który aktywnie działa w kierunku certyfikacji cyberbezpieczeństwa, rozwijając w ramach swojej działalności Jednostkę Certyfikującą. Polski producent może wystąpić o certyfikat w polskiej Jednostce Certyfikującej.

l Projekt KSO3C – Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria – jest współfinansowany na podstawie umowy CYBERSECIDENT/381282/II/NCBR/2018 przez Narodowe Centrum Badań i Rozwoju w ramach Programu CyberSecIdent. Projekt realizują Instytut Łączności, Instytut Technik Innowacyjnych EMAG z Sieci Badawczej Łukasiewicz oraz NASK Państwowy Instytut Badawczy odpowiedzialny za stworzenie Jednostki Certyfikującej wydającej certyfikaty.

cyberbezpieczeństwa[20]. Do certyfikacji systemów zarządzania bezpieczeństwem informacji stosuje się normę PN-EN ISO/IEC 27001[m], która (wzbogacona o inne z rodziny 27001) tworzy elastyczne ramy oceny i certyfikacji nie tylko systemów zarządzania bezpieczeństwem informacji, ale także ryzykiem. Obecnie w Polsce jest kilkanaście akredytowanych przez Polskie Centrum Akredytacji podmiotów[21], które wydają certyfikaty zgodności systemów zarządzania bezpieczeństwem informacji z normą PN-EN ISO/IEC 27001. Za normę 27001 i inne z tej rodziny odpowiada połączony Komitet Techniczny nr 1 ISO and IEC (JTC 1)[22].

Nadchodzące miesiące przyniosą wiele wyzwań w obszarze europejskiej certyfikacji cyberbezpieczeństwa. Akt o Cyberbezpieczeństwie stworzył ramy organizacyjne[n], które są obecnie operacjonalizowane na poziomie agencji ENISA[o] i Komisji Europejskiej. Agencja opublikowała właśnie propozycję pierwszego europejskiego programu certyfikacji cyberbezpieczeństwa (opartego o *Common Criteria*)[23]. Według zapowiedzi kolejne programy certyfikacji będą dotyczyć 5G, chmur obliczeniowych i IoT. Sama norma do certyfikacji IoT już istnieje (ETSI EN 303 645 z czerwca 2020 roku [24]).

Do publicznej konsultacji[25] przedstawiony został właśnie projekt pierwszego programu certyfikacji. Udział w konsultacjach publicznych to najprostsza z form włączenia się w prace normalizacyjne i certyfikacyjne. Warto śledzić ogłoszenia o naborach do tzw. *Ad-hoc Working Groups*[26]. Ze względu na szczególną rolę agencji ENISA w kształtowaniu reguł certyfikacji bezpieczeństwa ICT te grupy mają wyjątkowe znaczenie.

Technologie wydają się być niezależne od kontekstu regionalnego i politycznego. Specyfikacje techniczne Internetu Rzeczy czy sieci 5G są wspólne, nawet jeśli różnią się sposobem implementacji w lokalnych warunkach. Prace normalizacyjne, z definicji oparte na konsensusie, są miejscem szczególnego porozumienia „ponad podziałami". W międzynarodowych grupach roboczych organizacji normalizacyjnych wspólnie pracują specjaliści z Azji, Ameryki i Europy. To właśnie dlatego normy mają przed numerem oznaczenie literowe np. PN-EN ISO/IEC, w tym przykładzie podano najpełniejszy możliwy do osiągnięcia poziom zgodności krajowej, europejskiej i światowej. Takie oznaczenie normy świadczy o tym, że norma została przyjęta do stosowania przez organizacje międzynarodowe, została uznane za europejską i może być przywoływana w krajowych przepisach. Tempo adopcji norm jest tym szybsze, im więcej prac odbywa się w „połączonych komitetach". Można powiedzieć, że w świecie cyberbezpieczeństwa poziom współpracy międzynarodowej w obszarze normalizacji jest więcej niż zadawalający. Wyraźnie dowodzą tego wspólne projekty ISO, IEC, ETSI czy porozumienia takie jak

m Międzynarodowa Norma, która określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji.

n Akt o Cyberbezpieczeństwie powołał do życia Europejskie Ramy Cerfyfikacji Cyberbezpieczeństwa. Szczególną rolę w tworzeniu systemu certyfikacji uzyskała agencja europejska ENISA, niemniej każdy z krajów członkowskich został zobligowane do wyznaczenia National Cybersecurity Certification Authority (Krajowy Organ ds. Certyfikacji Cyberbepieczeństwa). Dodatkowo powołano do życia dwie struktury ECCG i SCCG – odpowiednio European i Stakeholders Cybersecurity Certificawtion Group – pierwsza w składzie oficjalnym delegatów rządów Państw członkowskich, druga wyłoniona w otwartym naborze przez ENISA, składająca się z reprezentatywnej próbki zainteresowanych przedstawicieli producentów, konsumentów i świata nauki. W Polsce trwają uzgodnienia i przygotowanie przepisów implementujących Akt, przy czym należy oczekiwać istotnej roli Ministerstwa Cyfryzacji. Podstawowym założeniem Europejskim Ram Certyfikacji jest powstanie (przygotowanie, uzgodnienie, przyjęcie) Europejskich Programów Certyfikacji Cyberbezpieczeństwa. Dotychczas żadnego programu nie przyjęto, ale pierwszy – oparty o normę Common Criteria (patrz dalej) – jest obecnie dostępny w wersji roboczej. Kolejne programy, których należy się spodziewać, to m.in. tematyka Internetu Rzeczy (IoT), chmury obliczeniowej (prace grupy roboczej Cloud Services Providers Certification – CSPCert), technologii 5G czy bezpieczeństwa systemów automatyki przemysłowej (w szczególności prace wykonane w ramach projektu ERNCIP). Bardziej szczegółowy program i harmonogram prac zostanie przyjęty w Rolling Work Programme, którego należy się spodziewać niebawem.

o Europejska Agencja ds. Cyberebzpieczeństwa.

CCRA (*Common Criteria Recognition Arrangement*). Osobnym zagadnieniem jest stosowanie wspólnych norm w przepisach europejskich i krajowych, gdzie widać wyraźnie, jak wiele zależy od lokalnego kontekstu, interesów i potrzeb.

SIECI 5G – *SECURITY BY DESIGN?*

Jednym z ciekawych przykładów budowania cyfrowej suwerenności w Europie jest próba normalizacji kwestii związanych z budową i rozwojem sieci mobilnych nowej generacji. Po pierwszych pilotażach i testowych instalacjach, od 2019 roku operatorzy telekomunikacyjni uruchamiają sieci 5G komercyjnie. Choć dla wielu europejskich operatorów na etapie planowania nowej, czy raczej rozbudowy starej sieci, naturalnym wyborem był i nadal jest sprzęt z dalekiej Azji, który łączy pewne istotne zalety technologiczne z przystępną ceną, to Europa podeszła do tego wyzwania w strategiczny sposób, właśnie w kontekście cyfrowej suwerenności.

W 2019 roku Komisja Europejska rozpoczęła proces szacowania ryzyka w sieciach 5G na poziomie krajowym[27], a następnie, 9 października 2019 roku, opublikowała dokument skoordynowanego podejścia do szacowania ryzyka w sieciach 5G na poziomie Unii Europejskiej (*EU coordinated risk assessment of the cybersecurity of 5G networks*[28]). Kolejnym etapem było opracowanie i opublikowanie 29 stycznia 2020 roku tzw. *Toolboxa* – dokumentu ***Cybersecurity of 5G networks EU Toolbox of risk mitigation measures***[29]. Podczas tych działań od początku wyraźnie wybrzmiewała teza, że szacowanie ryzyka i planowanie środków zaradczych musi, obok zagadnień technicznych, uwzględniać również kwestie strategiczne. Podkreślana była konieczność zachowania suwerenności cyfrowej państw członkowskich Unii Europejskiej, rozumianej zarówno w kontekście politycznym, jak i gospodarczym. Wskazano, że sieci piątej generacji (5G) będą w przyszłości stanowić niezbędną infrastrukturę cyfrową, łączącą dużą ilość urządzeń, obiektów i systemów, między innymi w krytycznych sektorach – energetyce, zaopatrzeniu i transporcie, służbie zdrowia, bankowości, a także w przemysłowych systemach sterowania, przenoszących wrażliwe informacje i wspierających systemy bezpieczeństwa.

Wszystkie te działania nie oznaczają niestety, że powstanie zunifikowane, bezpieczne europejskie 5G. Biorąc pod uwagę już rozpoczęte przez operatorów prace, ambitne ramy czasowe wdrożeń oraz fakt, że nowa technologia opiera się w znacznej mierze na już istniejącej infrastrukturze, nie osiągniemy niestety ujednoliconego stanu bezpieczeństwa sieci opartego na podejściu *(common European) security by design*. Dużym wyzwaniem na drodze do wspólnego podejścia są także utarte w każdym z krajów czy u każdego z operatorów ścieżki postępowania w zakresie kontraktowania elementów sieci, planów rozbudowy oraz lokalnej współpracy międzyoperatorskiej. Barierą w budowaniu niezależności i suwerenności opartej o stosowanie rozwiązań różnych producentów mogą być też przyzwyczajenia czy kompetencje inżynierskie preferujące określone rozwiązania technologiczne.

Dlatego wśród środków zaradczych wspomnianego *Toolboxa* wymieniane są takie aspekty jak wzmocnienie roli państwowych instytucji odpowiedzialnych za regulację rynku telekomunikacyjnego oraz bezpieczeństwo narodowe. Dokument podkreśla także istotność oceny ryzyka, zarówno na poziomie pojedynczego operatora, jak i w aspekcie ogólnokrajowym uwzględniającym wszystkich graczy rynkowych, potwierdzającą, czy nie dochodzi do uzależnienia od pojedynczego dostawcy. Kolejnym aspektem wskazanym wśród strategicznych środków zaradczych jest konieczność kontroli, czy nie dochodzi do wpływu państw spoza Unii Europejskiej na **integralność łańcucha dostaw komponentów sieci, konieczność audytu i kontroli tego, jakie rozwiązania są używane w krytycznych i wrażliwych segmentach sieci**, oraz konieczność oceny, z jakim ryzykiem wiąże się obecność w sieciach operatorskich technologii określonych, zwłaszcza pochodzących spoza Europy producentów. Taka ocena może być prowadzona zarówno z poziomu krajowego, jak i europejskiego. Dodatkowo niezwykle ważne jest zarządzanie strategią współistnienia różnych

dostawców, zarówno na poziomie operatorów, jak i infrastruktury przez nich współdzielonej, ale również na poziomie regionów geograficznych, zwłaszcza silnie urbanizowanych: monitorowanie transferu kapitału (ang. FDI – *Foreign Direct Investment*) i jego wpływu na produkcję elementów technologii 5G w Europie oraz troska o budowanie i rozwój europejskiego potencjału technologicznego w obszarze sieci nowych generacji.

Przy budowie 5G w Europie po raz pierwszy w historii powszechnej telefonii mobilnej, przy analizowaniu zagadnienia wydawałoby się tylko technologicznego i gospodarczego, tak wyraźnie wybrzmiewa troska, a nawet wyraźna obawa o suwerenność Europy – suwerenność opartą na technologiach cyfrowych. **Suwerenność ta postrzegana jest więc obecnie nie tylko w kontekście bezpieczeństwa danych, ale przede wszystkim technologii wykorzystywanej przy budowie sieci.** Jednym z istotniejszych działań w tym zakresie jest próba zmierzenia się z wyzwaniem, jakim jest wpisanie badania komponentów sieci 5G w opisany powyżej ekosystem certyfikacji w Europie. Proces już się rozpoczął – trwa analiza standardów technicznych, które opisują sieci 5G.

Zadania, które postawił *Toolbox*, mają też charakter techniczny. Wzmocnienie bezpieczeństwa fizycznego infrastruktury, wzmocnienie kontroli integralności oprogramowania oraz sformalizowanego zarządzania jego aktualizacją czy tzw. łataniem, podnoszenie standardów bezpieczeństwa w łańcuchu dostaw i jego uwzględnienie w procesie zakupowym, wykorzystanie i rozwój europejskich ram i programów certyfikacji dla krytycznych elementów sieci oraz wyposażenia klienckiego to tylko niektóre narzędzia zaproponowane przez *Toolbox*.

CYBERBEZPIECZEŃSTWO ŁAŃCUCHA WARTOŚCI

Rozważając kwestie cyberbezpieczeństwa w kontekście cyfrowej suwerenności, należy także uwzględnić kwestie łańcucha dostaw, czy też szerzej: **łańcucha wartości we współczesnym świecie technologii cyfrowych.** Każdy system ICT jest zbudowany z ogromnej ilości komponentów sprzętowych i programowych, a na każdy z komponentów sprzętowych składa się wiele elementów pochodzących od różnych producentów i dostawców. Każdy program komputerowy jest natomiast zbudowany z wielu modułów, wykorzystuje różne biblioteki i składa się z tysięcy linii kodu. Stopień skomplikowania systemów i liczba firm dostarczających poszczególne elementy systemów teleinformatycznych stale rośnie. Dlatego prawdziwym wyzwaniem staje się obecnie zapanowanie nad cyberbezpieczeństwem końcowego produktu czy usługi oferowanej użytkownikowi końcowemu. Coraz częściej więc **jednym z najpoważniejszych wyzwań bezpieczeństwa rozwiązań Przemysłu 4.0, IoT i sieci nowych generacji jest znalezienie skutecznego i możliwie wystandaryzowanego podejścia do zapewnienia cyberbezpieczeństwa w całym łańcuchu wartości** (ang. *value chain*), który składa się na końcowe produkty i usługi cyfrowe. Jak to z łańcuchami bywa, ich jakość (w tym przypadku bezpieczeństwo) zależy najczęściej od bezpieczeństwa najsłabszego ogniwa. Może nim być podatna biblioteka programistyczna, sterownik lub algorytm użyty przez jednego z dostawców jako komponent skomplikowanego systemu czy też element sprzętowy (np. pamięć) nieznanego producenta. Zdarza się, że niewielki fragment kodu *open source* jest używany masowo w milionach systemów i aplikacji. Dopiero po czasie wychodzi na jaw, że zawiera on krytyczną podatność, która pozwalała na obejście szyfrowania powszechnie używanego w internecie – to przypadek Heartbleed[p]. Jeszcze gorzej, jeśli powstające systemy opierają się na przestarzałych standardach, które nie zapewniają podstawowych wymogów bezpieczeństwa. To z kolei przykład standardu CAN Bus[30] opracowanego dla przemysłu motoryzacyjnego w latach osiemdziesiątych ubiegłego stulecia, a stosowanego w samochodach prawie wszystkich marek do dziś. Nie zapewnia on podstawowych mechanizmów bezpieczeństwa: uwierzytelnienia, szyfrowania, odporności na manipulacje. W internecie można znaleźć

p *The Heartbleed Bug*, [online:] https://heartbleed.com/

wiele dowodów na to, że w erze *connected cars* w prosty sposób, w prawie każdym samochodzie, można zablokować dowolne czujniki (np. parkowania lub zderzenia) podłączone – jak wszystkie urządzenia elektroniczne w aucie – do szyny CAN Bus.

Te przykłady ilustrują problem wykorzystywania komponentów, których poziom bezpieczeństwa jest nieznany lub zbagatelizowany. Brak świadomości lub postawienia odpowiednich wymogów (np. certyfikacji komponentów) albo trudność w przeanalizowaniu całego łańcucha dostaw i powiązań podwykonawczych powoduje, że użytkownik produktu końcowego lub usługi nie ma wiedzy ani świadomości na temat ryzyka, na jakie jest narażony w czasie eksploatacji.

W kilku krajach istnieją opracowania, standardy, rekomendacje czy dobre praktyki dotyczące zarządzania ryzykiem w kontekście cyberbezpieczeństwa łańcucha, publikowane przez znane ośrodki czy agencje, takie jak amerykańskie NIST, CISA, brytyjskie NCSC, australijskie ACSC czy agencja UE ENISA. Jeden z najciekawszych przykładów całościowego podejścia do tego zagadnienia, który został zidentyfikowany przez wspomniany zespół, to inicjatywa japońskiego Ministerstwa Gospodarki, Handlu i Przemysłu METI (*Ministry of Economy, Trade and Industry*).

W ramach japońskiej inicjatywy CPSF[31], opublikowanej w roku 2019, która wpisuje się w krajowe strategie *Society 5.0* oraz *Connected Industries*, problem zarządzania bezpieczeństwem łańcucha dostaw jest ważnym elementem całościowego podejścia do cyberbezpieczeństwa oraz bezpieczeństwa fizycznego w świecie nowoczesnych technologii. Dokument zawiera zestaw rekomendowanych środków zapewniających bezpieczeństwo, które są wymagane dla wdrożenia w przemyśle. Główne cele przyświecające japońskiej inicjatywie to z jednej strony standaryzacja wymagań dotyczących zarządzania bezpieczeństwem łańcucha dostaw, z drugiej zaproponowanie nowego podejścia do bezpieczeństwa IT przez pryzmat łańcucha dostaw.

Co ciekawe, w podejściu japońskim znajdziemy mapowanie do innych znanych standardów czy zaleceń, takich jak NIST, *Common Criteria*, COBIT 5, ISO/IEC 27001:2013. Wydaje się, że dokumenty opracowane przez japońskie Ministerstwo Gospodarki, Handlu i Przemysłu mogą być dobrym punktem odniesienia do opracowania polskich wymagań dotyczących zarządzania łańcuchem dostaw w kontekście cyberbezpieczeństwa. Wśród zalet podejścia zaproponowanego przez rząd Japonii można wymienić:

- kompleksowe podejście do budowy systemu bezpieczeństwa uzupełniające i rozszerzające inne wytyczne, zawierające zestaw spójnych i jasnych wymagań wraz z przykładami rozwiązań i zabezpieczeń;
- uwzględnienie specyfiki poszczególnych obszarów/typów technologii, np. IoT, oprogramowanie;
- odniesienia do powszechnych standardów i wytycznych;
- wymagania możliwe do zastosowania zarówno w sektorze publicznym, jak i prywatnym.

Niestety nie jest łatwo wskazać, jak systemowo radzić sobie z problemami cyberbezpieczeństwa łańcucha wartości. Wyzwanie, jakim jest analiza dostępnych w świecie, m.in. tych wymienionych powyżej, dobrych praktyk w systemowym podejściu do cyberbezpieczeństwa łańcucha, zostało podjęte w Polsce w ramach prac Grupy ds. Cyberbezpieczeństwa Ministerstwa Cyfryzacji[q], gdzie pracuje zespół ekspercki ds. cyberbezpieczeństwa łańcucha dostaw.

q Zespół został powołany w 2017 roku, a w jego skład wchodzą przedstawiciele administracji, ośrodków akademickich oraz sektora prywatnego.

PODSUMOWANIE

Rozwój technologii wymusza na poszczególnych państwach i organizacjach międzynarodowych coraz większe zainteresowanie kwestiami suwerenności cyfrowej. Zagadnienie to ma bardzo wiele aspektów, zaczynając od samej interpretacji i prawnej definicji tego, czym jest cyfrowa suwerenności i jak może być determinowana. W ostatnim czasie, jednym z jej istotniejszych wyznaczników i przejawów są kwestie technologiczne oraz związana z nimi normalizacja, standaryzacja i certyfikacja. W obliczu silnej pozycji pozaeuropejskich dostawców technologii, Europa stara się tworzyć takie ramy, które pozwolą zapewnić odpowiedni poziom bezpieczeństwa. Warto przy tym zauważyć, że chociaż praca nad normami, standardami i certyfikacją przebiega w międzynarodowej atmosferze i jest w pewnym sensie niezależna od aspektów strategicznych czy politycznych, to sama ich implementacja jest silnie powiązana z interesami poszczególnych państw i w pewien sposób może ograniczać poszczególne rynki – dopuszczane będą tylko certyfikowane produkty i usługi. W tym aspekcie niezwykle istotne jest też zapewnienie bezpiecznego łańcucha dostaw, silnie akcentowane przez UE i państwa członkowskie. Kwestie te bardzo wyraźnie uwypukliła pandemia COVID-19, podczas której bardzo wyraźnie widać, jak istotne jest zapewnienie cyberbezpieczeństwa w całym łańcuchu dostaw.

Współfinansowane przez instrument UE „Łącząc Europę". Odpowiedzialność za treść niniejszej publikacji ponosi NASK i niekoniecznie odzwierciedla ona opinię Unii Europejskiej.

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę"

PRZYPISY

1 *Shaping Europe's digital future*, European Commission, s. 3.

2 *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013*, Parlament Europejski i Rada UE, 17.04.2019, [online:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32019R0881.

3 *Island of Palmas Arbitral Award*, 04.04.1928, s. 838, [online:] https://legal.un.org/riaa/cases/vol_II/829-871.pdf.

4 Gueham F., *Digital Sovereignty*, Foundation Pour L'Innovation Politique, 01.2017.

5 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, Parlament Europejski i Rada UE, 06.07.2016, [online:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016L1148&from=PL.

6 *Tallinn Manual 2.0 on the International Law application to Cyber Operations*; Międzynarodowa Grupa Ekspertów, Cambridge University Press, Cambridge, 2017.

7 Tamże, s. 12-13.

8 Tamże, s. 15.

9 Tamże, s. 16.

10 Tamże, s. 16.

11 Tamże, s. 19.

12 *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013*, Parlament Europejski i Rada UE, 17.04.2019, [online:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32019R0881.

13 *Co to jest PN?*, Polski Komitet Normalizacyjny, 2020, [online:] https://www.pkn.pl/polskie-normy/informacje-o-pn/co-jest-pn.

14 *Dobrowolność stosowania norm*, Polski Komitet Normalizacyjny, 2020, [online:] https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn.

15 *Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE*, Parlament Europejski i Rada UE, 25.10.2012, [online:] http://data.europa.eu/eli/reg/2012/1025/2015-10-07.

16 *Techniques for assurance of digital material used in legal proceedings*, ETSI, ETSI TS 103 643, 01.2020, [online:] https://www.etsi.org/deliver/etsi_ts/103600_103699/103643/01.01.01_60/ts_103643v010101p.pdf.

17 *Mutual Recognition Agreement of Information Technology Security Certificates*, SOGIS, 08.01.2010, [online:] https://www.sogis.eu/.

18 *Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security*, CCRA, 02.07.2014, [online:] https://www.commoncriteriaportal.org/ccra/.

19 *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*, Rada Ministrów, 12.04.2012, [online:] http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20120000526.

20 *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Rada Ministrów, 06.07.2018, [online:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560.

21 *Jednostki certyfikujące systemy*, Polskie Centrum Akredytacji, 2020, [online:] https://www.pca.gov.pl/akredytowane-podmioty/akredytacje-aktywne/jednostki-certyfikujace-systemy/szukaj.html?fraza=27001.

22 Joint Technical Commitee (JTC 1), 2020, [online:] https://jtc1info.org/.

23 *Cybersecurity Certification: EUCC Candidate Scheme*, ENISA, 02.07.2020, [online:] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

24 Antipolis S., *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*, ETSI, ETSI EN 303 645, 30.06.2020, [online:] https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard.

25 *ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme*, ENISA, 02.07.2020, [online:] https://www.enisa.europa.eu/news/enisa-news/enisa-launches-public-consultation-for-first-candidate-cybersecurity-certification-scheme.

26 *DECISION NO MB/2019/11 of the Management Board of the European Union Agency For Cybersecurity on the Establishment and Operation of Ad Hoc Working Groups For European Cybersecurity Certification Scheme*, ENISA, 11.2019, [online:] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202019_11%20on%20ad%20hoc%20working%20groups%20on%20certification%20schemes.pdf.

27 *A common EU approach to the security of 5G networks*, *European Commission*, 26.03.2019, [online:] https://ec.europa.eu/commission/news/common-eu-approach-security-5g-networks-2019-mar-26_pl.

28 *Member States publish a report on EU coordinated risk assessment of 5G networks security*, European Commission, 09.10.2019, [online:] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

29 *Secure 5G networks: Questions and Answers on the EU toolbox*, European Commission, 29.01.2020, [online:] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

30 Hartzell S., Stubel C., *Automobile CAN Bus Network Security and Vulnerabilities*, University of Washington

31 *Cyber/ Phisical Security Framework*, METI, 18.04.2019, [online:] https://www.meti.go.jp/english/press/2019/0418_001.html.

Tomasz Dylik

GEOPOLITYKA CYFROWYCH PASÓW I SZLAKÓW

GEOPOLITYCZNA ROLA INTERNETU

Geopolityka infrastruktury cyfrowej opiera się na dwóch przeciwstawnych kierunkach politycznych, ponieważ z jednej strony opiera się na poszczególnych państwach, takich jak USA lub Chiny (ale także na podmiotach ponadnarodowych takich jak np. Unia Europejska), z drugiej obejmuje zdecentralizowane sieci transnarodowe[1]. Podział ten zmusza czasem państwa do brania pod uwagę nie tylko kryterium opłacalności, ale także ryzyka politycznego (ang. *political risk*) w rozwoju swojej infrastruktury cyfrowej. Wynika to z postrzegania cyfrowej suwerenności jako elementu składowego bezpieczeństwa narodowego. Warto tu zwrócić uwagę, że przodkiem Internetu był projekt wojskowy ARPANET wykorzystywany przez armię USA, który następnie rozszerzono na amerykańskie uniwersytety i tam dostrzeżono jego potencjał biznesowy. Wraz z rozwojem Internetu pojawiły się również firmy technologiczne, które zdolne są do wykorzystania swojej pozycji nie tylko do generowania ogromnych zysków, ale również do prowadzenia własnej polityki i działań paradyplomatycznych.

Geopolityka Internetu odnosi się przede wszystkim do fizycznej warstwy sieci, którą tworzy infrastruktura cyfrowa, czyli wszystkie systemy technologiczne, które umożliwiają tworzenie, przesyłanie i zbieranie danych cyfrowych. Są to m.in. podmorskie i naziemne kable, urządzenia cyfrowe, centra danych, satelity, routery, i wszystkie inne ulokowane w przestrzeni zasoby niezbędne do funkcjonowania komunikacji cyfrowej. Tworzą one opasającą Ziemię sieć połączeń, która biegnie wzdłuż geograficznych i politycznych podziałów świata. Jako taka odgrywa ona rolę w geopolitycznej rywalizacji państw.

O przewadze technologicznej danego kraju decyduje infrastruktura i dostęp do zasobów koniecznych do jej wykorzystania. Infrastruktura cyfrowa, w tym jej nasycenie i położenie światłowodów, należą do czynników determinujących obieg danych i stanowią szkielet Internetu. Mocarstwa światowe wykorzystują cyberprzestrzeń jako instrument i forum do realizacji swoich interesów zarówno w polityce wewnętrznej, jak i zewnętrznej, co szerzej opisane jest w rozdziale 13 niniejszego raportu. Gwałtowny rozwój Internetu oraz technologii informacyjnych wymusza rolę bezpieczeństwa i niezależności funkcjonowania sieci. Pojawiają się postulaty ograniczenia dostępu do sieci określonym podmiotom albo w formie inicjatyw międzynarodowych (np. Propozycje Praskie, inicjatywa Clean Network), albo narodowych (chiński Wielki Firewall, rosyjski RuNet).

GEOSTRATEGICZNE ZNACZENIE DRÓG CYFROWYCH

Pomimo powszechnego dostępu do Internetu i cyberprzestrzeni precyzyjne pojmowanie sposobu ich działania jest nader rzadkie. Internet istnieje i funkcjonuje dzięki złożonej infrastrukturze fizycznej o zasięgu ogólnoświatowym: m.in. kable światłowodowe, centra danych, systemy komputerowe i kontrolery. Pomimo tego, że Internet w obecnym kształcie nie ma narodowości[a], to powszechny dostęp do niego może być ograniczany, m.in. na terytorium konkretnych państw. Dostęp do Internetu pozostaje w praktyce pod kontrolą rządów poszczególnych krajów, które sprawują suwerenną władzę w obrębie swoich granic, w ramach których funkcjonują operatorzy czy producenci sprzętu i usług cyfrowych, a także w ramach których ulokowana jest infrastruktura cyfrowa, niezbędna do przesyłu danych. Przykładem może być niedawne

a Co jednak nie odnosi się wprost do cyberprzestrzeni, która może obejmować np. wspólnotę opartą na języku np. czeską, czy polską.

ograniczenie dostępu do Internetu obywatelom Białorusi wskutek protestów po wyborach prezydenckich w sierpniu 2020 r.[2].

Mimo tego, że światłowody nie są jedyną możliwością przesłania sygnału internetowego, to znaczna (w 2018 r. ich wykorzystanie stanowiło średnio ok. 26% według danych OECD[3]) część danych przekazywana jest właśnie tą drogą. Alternatywą pozostaje łączność satelitarna, która jest dobrym rozwiązaniem jako prawdziwie niezależny *backup*, jednak zdecydowana większość ruchu przesyłana poprzez kable światłowodowe (ok. 99% dla podmorskich międzykontynentalnych światłowodów[4]) stanowiące rdzeń sieci łączący poszczególne kontynenty. Warto tu zauważyć, że wzrost popytu na pasmo wynika m.in. z migracji usług do rozwiązań chmurowych oraz stałego rozwoju rynku mobilnego (również poprzez wdrażanie technologii 5G). Taka ilość ruchu wymaga zwiększania pojemności szkieletu Internetu i poszukiwania nowych rozwiązań dla zwielokrotnienia pojemności transmisji przy wykorzystaniu istniejącej infrastruktury – obecnie na całym świecie pracuje nieco ponad 400 kabli podmorskich o łącznej długości ponad 1,2 mln kilometrów[5].

Poszczególne szlaki i połączenia są dobrze znane i na przestrzeni wieków wykorzystywane były do żeglugi i wymiany towarów, dziś służą również do wymiany danych. Najważniejsze połączenia podmorskie biegną przez Atlantyk (Europa–USA), Pacyfik (USA–Japonia, USA–Azja Płd.-Wsch.), czy w regionie europejskim – Morze Śródziemne. Nie bez znaczenia pozostają kable ziemne łączące poszczególne kraje i kontynenty – jednym z głównych przykładów są kable tranzytowe na terytorium Polski łączące Europę Zachodnią z Rosją i Dalekim Wschodem. W przeszłości ten, kto kontrolował szlak handlowy, wykorzystywał to do rozwoju – m.in. miast i ośrodków handlowych – analogiczna sytuacja dotyczy cyfrowych szlaków, obecnie przyczyniają się one do rozwoju centrów danych, technologii i kompetencji obywateli, przyspieszając modernizację gospodarczą i przyciągając inwestorów.

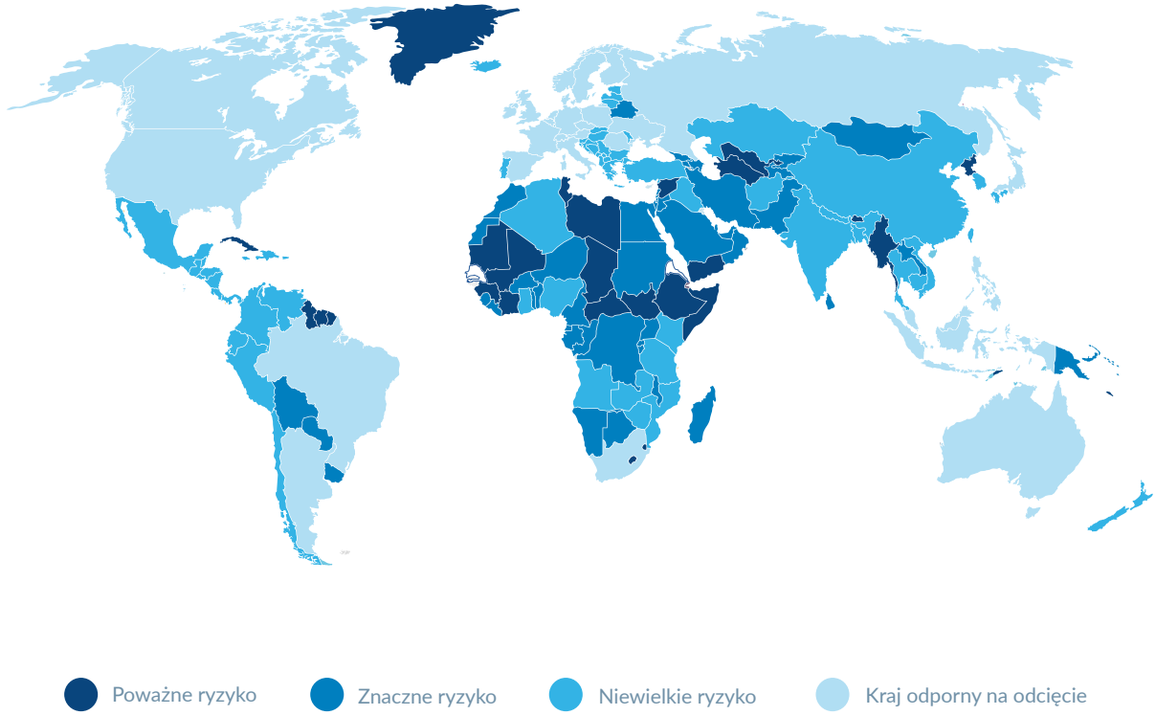
Niezawodność i ciągłość działania dróg cyfrowych na świecie w dużej mierze zależy od niezawodności kabli światłowodowych. Nieprzerwana transmisja ma strategiczne znaczenie dla funkcjonowania Internetu w danym regionie – światłowody jak każdy element infrastruktury fizycznej są narażone na awarie i uszkodzenia, również te zamierzone. Straty związane z utratą łączności dotyczą nie tylko użytkowników końcowych, ale przede wszystkim instytucji publicznych czy bankowych, a niedostępność usług może wiązać się z ogromnymi stratami finansowymi. Zagrożenie związane z przerwaniem transmisji rośnie szczególnie w przypadku newralgicznych punktów, gdzie znajduje się wiele kabli światłowodowych – zarówno w przypadku kabli podmorskich, jak i ziemnych. Miejsca koncentracji światłowodów często są wymuszone przez warunki geograficzne (np. cieśniny), bądź warunki fizyczne ułatwiające instalację i eksploatację (określone trasy kabli na dnie oceanów).

Mimo specjalnych zabezpieczeń znane są przypadki, gdzie całe kraje i regiony zostawały odcięte od światowych zasobów sieci. W 2011 r. 75-letnia obywatelka Gruzji zniszczyła kabel światłowodowy w okolicach Tbilisi – w wyniku tego działania w sąsiedniej Armenii sieć została odcięta na 5 godzin, a część mieszkańców Gruzji i Azerbejdżanu odczuwała problemy w dostępie do sieci[6]. Trzy lata wcześniej w styczniu 2008 r. awarii uległy dwa kable podmorskie SEA-ME-WE4 oraz FLAG EA biegnące na dnie Morza Śródziemnego pomiędzy Egiptem a Włochami. Ta relacja odpowiadała wtedy za ok. 90% transmisji pomiędzy Europą a Bliskim Wschodem (pośrednio również z Indiami). Łącznie na przełomie stycznia i lutego 2008 r. uszkodzonych zostało pięć podmorskich kabli w rejonie Morza Śródziemnego. Zgodnie z raportem France Telecom podanym przez serwis Wired[7], skutki tych awarii były odczuwalne w co najmniej 14 krajach: w 100% odcięte zostały Malediwy, następnie problemy z łącznością występowały na terenie Indii, Kataru, Dżibuti, Zjednoczonych Emiratów Arabskich czy Egiptu i Arabii Saudyjskiej. Ryzyko potencjalnej awarii wywołało zaniepokojenie i dyskusję nad

bezpieczeństwem obecnego szkieletu Internetu opartego na kablach podmorskich.

Według badań z 2012 r. firmy Renesys specjalizującej się w analizie topologii sieci wiele krajów posiada jednego lub dwóch operatorów zapewniających komunikację ze światem oznaczonych jako kraje wysokiego ryzyka odcięcia (oznaczone kolorem ciemnozielonym na mapie poniżej, m.in. Mauretania, Kuba czy Uzbekistan). Kolejna kategoria oznaczona jako znaczące zagrożenie odcięciem od sieci obejmuje liczne kraje, które posiadają od dwóch do 10 operatorów sterujących ruchem zewnętrznym (m.in. Białoruś, Paragwaj czy Egipt). Powyższe dane pokazują, że mimo powszechności dostępu do Internetu kilkadziesiąt państw na świecie może stosunkowo łatwo zostać odciętych od cyberprzestrzeni, co w znacznym stopniu zdestabilizowałoby funkcjonowanie państwa.

RYSUNEK 1.
RYZYKO ODCIĘCIA KRAJU OD ZASOBÓW ŚWIATOWEGO INTERNETU
(stan na 11.2012)



Źródło: *Renesys*, 09.2012[8].

Europa Środkowo-Wschodnia posiada stabilny fizyczny dostęp do globalnej sieci poprzez światłowody, stąd wydawać by się mogło, że groźba odcięcia od cyberprzestrzeni jest praktycznie niemożliwa. Należy jednak pamiętać, że zdecydowana większość połączeń wychodzących z tego regionu realizowana jest poprzez kable światłowodowe zbudowane bądź będące własnością krajów sąsiednich, a w przypadku kryzysu czy awarii region EŚW pozostaje w tej kwestii w relacji zależności od krajów sąsiedzkich. To sytuacja analogiczna do dystrybucji i przesyłu gazu – w przypadku kryzysu kraje przesyłowe posiadają techniczne możliwości do zakłócenia dostępu do cyberprzestrzeni. Analiza mapy światłowodowej pokazuje, że kraje Europy Zachodniej z dostępem do morza mają zapewnione awaryjne podmorskie połączenia światłowodowe. Dlatego (tak jak w przypadku gazoportów, które mogą zapewnić odpowiednią niezależność) konieczna jest budowa własnego i niezależnego połączenia światłowodowego do zasobów Internetu. Dobrym kierunkiem wydaje się Ameryka Północna i Stany Zjednoczone. Ten kraj jest odpowiednio zabezpieczony przed próbami zakłócenia łączności, a dodatkowo pełni funkcję hubu dla połączeń w każdym innym kierunku.

Niezależność i bezpieczeństwo infrastruktury fizycznej są kluczowe dla nieprzerwanej obecności w cyberprzestrzeni, nie należy jednak zapominać o innym ważnym aspekcie tj. niezależności infrastruktury w kontekście własnościowym. Kontrola nad rzeczywistymi i cyfrowymi szlakami uwarunkowana jest przez szereg czynników, w tym przez położenie geograficzne danego państwa, ale również przez kwestię własności infrastruktury. Mocarstwa oraz korporacje mają świadomość, że rozszerzenie swojej strefy wpływów w cyberprzestrzeni i realnym świecie można osiągnąć na wiele sposobów – jednym z najskuteczniejszych jest inwestowanie w infrastrukturę danego regionu.

Mimo powojennej dekolonizacji świat wciąż podzielony jest na strefy wpływów, jednak są to częściej więzy gospodarcze, biznesowe i finansowe. Jednym z bardziej ogólnych przykładów tego jest zaangażowanie mocarstw w różnych rejonach świata – dla przykładu w ciągu ostatnich 15 lat suma chińskich inwestycji w Afryce przekroczyła łączne inwestycje USA, Francji i Wielkiej Brytanii, a przywódcy afrykańscy otrzymują kolejne propozycje pożyczek i pomocy finansowej ze strony Państwa Środka. Zagraniczne inwestycje bezpośrednie (ang. *Foreign Direct Investments*, *FDIs*) dotyczą wszystkich obszarów – infrastruktura drogowa, przesyłowa, fabryki, usługi i dodatkowo udzielanie gigantycznych pożyczek państwom. Można przypuszczać, że niektóre obszary, w tym np. Afryka, są dla Chin także próbą przed rozpoczęciem ekspansji gospodarczej na wielką skalę w kolejnych regionach świata. Dobrym przykładem zaawansowanych już działań Państwa Środka jest Chińska Inicjatywa Pasa i Drogi – na którą składa się m.in. stworzenie pasa gospodarczego wzdłuż historycznego Jedwabnego Szlaku, która za zadanie ma zbudowanie nowoczesnych połączeń wzdłuż kontynentu eurazjatyckiego. W ramach tego projektu powołana została grupa „17+1" skupiająca Polskę i inne kraje Europy Środkowo-Wschodniej, która dla Chin pozostaje bramą do Europy Zachodniej i tu starają się zwiększyć swoje wpływy gospodarczo-polityczne. Podobnie jak w przypadku twardej infrastruktury, Polska i inne kraje Europy Środkowo-Wschodniej pozostają bramą do Europy Zachodniej dla transmisji danych – obecnie to właśnie tą drogą biegną najkrótsze połączenia wschód–zachód. Utrzymanie tej pozycji pozostaje dużym wyzwaniem dla naszego regionu, szczególnie w sytuacji doniesień o planach budowy połączenia światłowodowego z Japonii do Finlandii wzdłuż wybrzeża Rosji, co w połączeniu z już istniejącym kablem Finlandia–Niemcy może stanowić dużą konkurencję. Jednak umiejętne wykorzystanie własnego położenia na skrzyżowaniu dróg optycznych (światłowodów) z Azji, Bliskiego Wschodu, Europy Zachodniej i Północnej powinno stanowić dodatkowy atut.

Wspólne inwestycje w rozwój sieci telekomunikacyjnych – poprzez m.in. projekt „3 Seas Digital Highway", który jest częścią Inicjatywy Cyfrowego Trójmorza, umożliwią swobodny przepływ danych

i w pewnej części wyeliminuje konieczność dublowania infrastruktury dochodzącej do wysp danych w całym regionie. Realizacja tego projektu stworzy odpowiednie warunki dla rozwoju gospodarki opartej na danych i uatrakcyjni region jako miejsce, w którym przesyłane dane są terminowane, a nie jedynie przesyłane dalej. Dodatkowym atutem jest możliwość zbudowania zintegrowanych systemów powiadamiania z niezbędnymi elementami cyberbezpieczeństwa, które zwiększą poziom bezpieczeństwa na nowe transgraniczne zagrożenia o charakterze hybrydowym.

Początkowo duże inwestycje w podmorską sieć szkieletową były domeną poszczególnych państw bądź konsorcjów operatorów narodowych (m. in. British Telecom/France Telecom wspólnie z AT&T w latach 70. XX w.). Obecnie główni gracze na arenie międzynarodowej to tzw. OTT (ang. *Over-The-Top*), firmy pierwotnie odpowiedzialne za dostarczenie danych oraz terminali abonenckich, które rozszerzają teraz swoje strefy wpływu nie tylko w świecie wirtualnym, ale również rzeczywistym poprzez inwestycje w kable podmorskie czy budowę gigantycznych centrów danych w dotychczas mniej rozwiniętych regionach. Współczesny „wyścig zbrojeń" o dominację w dziedzinie cyberprzestrzeni wymaga ciągłego rozwoju – a ten, kto pozostaje w miejscu, traci. Niestety już na starcie tego wyścigu region Europy przegrywa. Przyjęta taktyka forsowania utworzenia paneuropejskiego operatora telekomunikacyjnego, który miałby tendencje do działania w wymiarze globalnym, może nie być wystarczająca.

REKOMENDACJE DLA POLSKI I REGIONU TRÓJMORZA

Kształt cyberprzestrzeni na najbliższe 15–30 lat ustala się właśnie teraz – odpowiednie wykorzystanie własnych zasobów pozwoli na zajęcie lepszej pozycji w przyszłym układzie sił. Jak w takiej sytuacji mogą odnaleźć się kraje, w tym Polska, które nie mogą konkurować z gigantami cyberprzestrzeni pod względem wielkości inwestycji czy obecnego wpływu na cyberprzestrzeń? Cały region Europy Środkowo-Wschodniej, w szczególności region Trójmorza na czele z Polską, musi wykazać się intensyfikacją działań i myśleniem perspektywicznym. Z jednej strony konieczne jest dalsze wykorzystywanie atutu w postaci położenia geograficznego i dalsze rozwijanie przesyłu ruchu internetowego na linii wschód–zachód poprzez wzmacnianie pozycji krajów będących „Bramą do Europy". Z drugiej strony budowa niezależnego połączenia światłowodowego do Stanów Zjednoczonych[b], przy jednoczesnym rozwijaniu sieci zapewniającej dostęp do Morza Śródziemnego i Bliskiego Wschodu, pozwoli na rozwój łączności na linii południkowej i otworzenie się na nowe rynki w cyberprzestrzeni.

Odpowiednie inwestycje w kształtowanie infrastruktury cyfrowej poprzez inwestycje w obszarze szkieletowym, m. in. przez wspomniany projekt tzw. Cyfrowej Autostrady Trójmorza („3 Seas Digital Highway"), czyli sieci połączeń cyfrowych między państwami regionu, jak i dostępowym, w przyszłości uzupełnione o technologię 5G, pozwoli zmniejszyć dystans wschodzących krajów Europy Środkowo Wschodniej do partnerów ze „Starej Europy", jednocześnie realizując założenia Jednolitego Rynku Cyfrowego. Uzupełnieniem do rozwoju twardej infrastruktury pasywnej powinno być rozwijanie własnych rozwiązań technologicznych i produkcji urządzeń w celu uniezależnienia się od dużych producentów sprzętu. Dodatkowo budowa zintegrowanych systemów zarządzania kryzysowego i cyberbezpieczeństwa w oparciu o własną infrastrukturę pasywną i aktywną, wzmocnią region przed zagrożeniami współczesnego świata o charakterze hybrydowym.

b Nazwą proponowaną dla tego światłowodu przez Instytut Kościuszki jest „3Seas1Ocean".

PRZYPISY

1 *Das Zeitalter der digitalen Geopolitik*, Internationale Politik und Gesellschaft, 05.07.2019, [online:] https://www.ipg-journal.de/rubriken/aussen-und-sicherheitspolitik/artikel/das-zeitalter-der-digitalen-geopolitik-3579/.

2 *Belarus: Internet Disruptions, Online Censorship*, Human Rights Watch, 28.07.2020, [online:] https://www.hrw.org/news/2020/08/28/belarus-Internet-disruptions-online-censorship.

3 *1.10. Percentage of fibre connections in total broadband*, OECD, 2019, [online:] https://www.oecd.org/sti/broadband/broadband-statistics/

4 *Underwater Cloud: Inside the Cables Carrying 99% of Transoceanic Data Traffic*, 99%invisible, 30.06.2017, [online:] https://99percentinvisible.org/article/underwater-cloud-inside-cables-carrying-99-international-data-traffic/.

5 *Submarine Cable 101*, Telegeography, 2020, [online:] https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

6 *Georgian Woman Accidentally Brings Down Armenia's Internet*, IEEE Spectrum, 2011, [online:] https://spectrum.ieee.org/riskfactor/telecom/internet/georgian-woman-accidentally-brings-down-armenias-internet.

7 *Undersea Cables Cut; 14 Countries Lose Web – Updated*, Wired, 2008, [online:] https://www.wired.com/2008/12/mediterranean-c/.

8 *What's Your Country's Risk of Internet Blackout?*, the Atlantic, 30.11.2012, [online:] https://www.theatlantic.com/technology/archive/2012/11/whats-your-countrys-risk-of-Internet-blackout/265790/.

Dr hab. Teodor Buchner

PRZESTRZEŃ KOSMICZNA I CYFROWY WYŚCIG ZBROJEŃ

ZNACZENIE I CHARAKTERYSTYKA TECHNOLOGII KOSMICZNYCH

Kosmos potrafi od lat rozpalać ludzką wyobraźnię, napędzać marzenia i plany biznesowe, budzić emocje w skali społecznej, których zakres rozciąga się od dumy narodowej, podziwu i wspólnego przeżycia momentu dziejowego (jak przy lądowaniu na Księżycu) przez poczucie bezpieczeństwa lub zagrożenia (jak po wystrzeleniu Sputnika) do rozpaczy i współczucia (jak po katastrofie Challengera). Rządy wszystkich krajów potrzebują tych zbiorowych emocji do umacniania wspólnot narodowych i tworzenia ikonicznych zdjęć startów i lądowań oraz punktów odniesienia, takich jak Sputnik, Łajka lub program Apollo, i ikon jak Gagarin, Armstrong, Tierieszkowa czy Mirosław Hermaszewski. Uczestnicy amerykańskiego programu kosmicznego do dziś biorą udział w konferencjach, opowiadając o amerykańskim micie i głosząc pochwałę wspólnoty, pragmatyzmu i organizacji.

Wyścig kosmiczny napędza rozwój gospodarczy podobnie jak wojna czy budowa akceleratorów cząstek i komputerów kwantowych. Własna technologia dzięki efektowi dyfuzji napędza kolejne obszary gospodarki. W grupie technologii kosmicznych znajdują się między innymi:

- inżynieria materiałowa (projektowanie płytek, które nie spłoną na skutek tarcia atmosferycznego[1]),
- inżynieria mechaniczna (konstrukcja musi stawić czoła ekstremalnym zmianom temperatur podczas dnia i nocy, które w zależności od orbity mogą sięgać nawet kilkuset stopni, oraz drganiom podczas startu, gdy przyspieszenia przekraczają kilkukrotnie przyspieszenie ziemskie),

- elektronika (musi znosić ekstremalne temperatury oraz twarde promieniowanie kosmiczne),
- optoelektronika (ogniwa paliwowe, systemy obrazowania),
- radioelektronika (anteny, obrazowanie radarowe)
- i fizyka (czujniki).

Kolejny obszar technologii otwiera się na Ziemi w związku z rozwojem sposobów wykorzystania danych satelitarnych i poszukiwaniem nowych modeli użycia i nisz rynkowych. Takie dziedziny gospodarki jak telekomunikacja, rolnictwo precyzyjne, gospodarka leśna, geologia i górnictwo, kartografia dla inwestycji, nawigacja, meteorologia o wysokiej precyzji, ochrona środowiska, gospodarka wodna, ale także bezpieczeństwo narodowe, bezpieczeństwo żeglugi morskiej i powietrznej, bezpieczeństwo konstrukcji, w tym dróg i mostów, zarządzanie kryzysowe, radioelektronika (instalacje naziemne) zyskały dzięki technologiom kosmicznym nowy wymiar i stoją przed nowymi wyzwaniami dla swojego rozwoju. Także różne dziedziny nauki: astronomia, klimatografia, glacjologia czy oceanografia otrzymują szeroki strumień danych, które powiększają stan wiedzy, co nierzadko przekłada się na nowe technologie i ich zastosowania, a to napędza rozwój gospodarczy.

Do obsługi tych dziedzin gospodarki służy ponad 2600 satelitów, w szczególności satelity służące do obserwacji Ziemi, które dostarczają zobrazowań satelitarnych, ale również satelity telekomunikacyjne, których zadaniem jest tzw. radiodyfuzja – rozproszenie sygnału otrzymanego z anteny nadawczej na duży obszar, tak aby sygnał docierał jednocześnie do szerokiego kręgu odbiorców. Ponadto wyróżnia się satelity nawigacyjne, satelity badawcze zajmujące się badaniem Ziemi i Kosmosu za pomocą rozlicznych czujników (ang. *remote sensing*) oraz wiele satelitów testowych, których zadaniem jest przeprowadzanie rozmaitych badań przemysłowych.

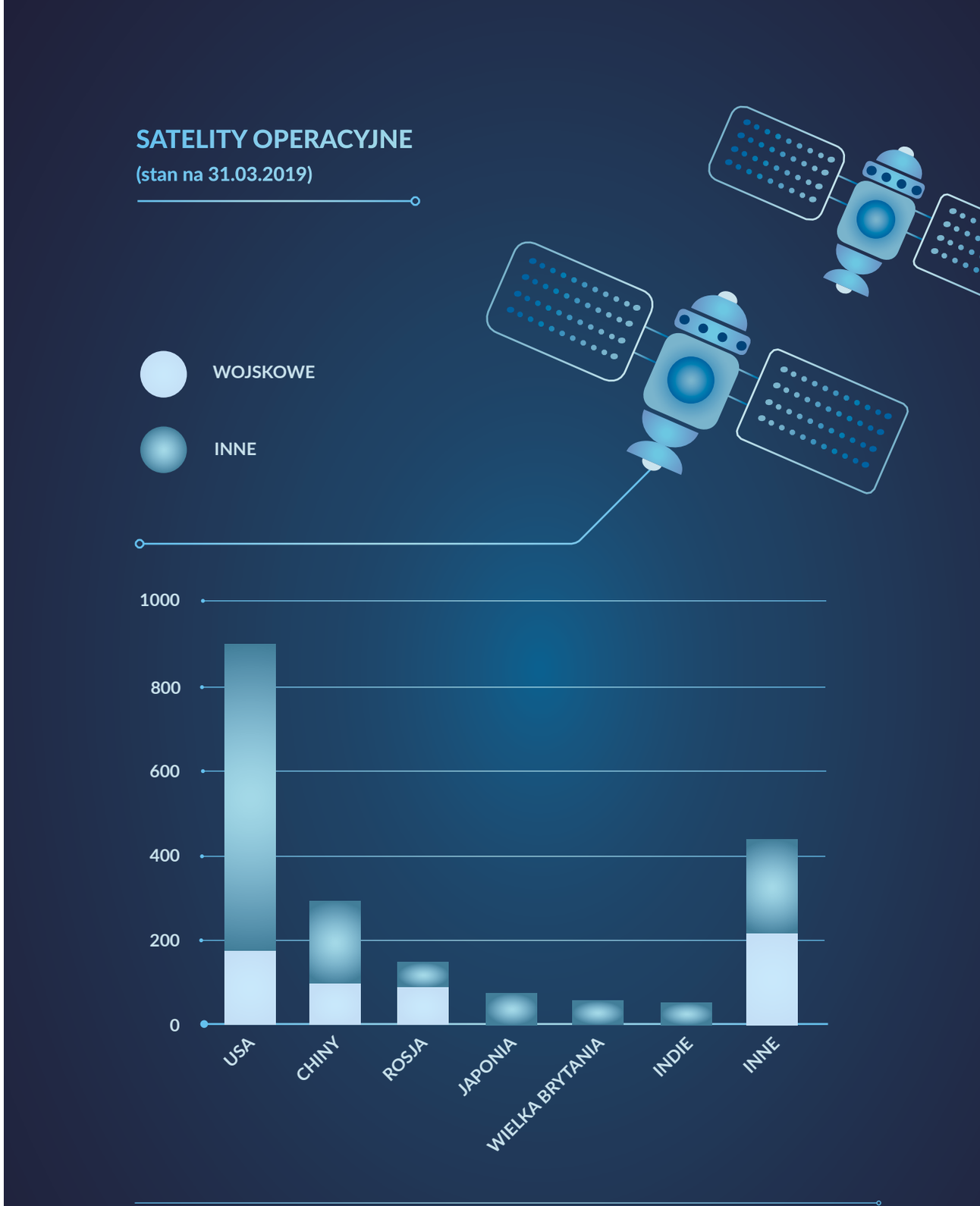
2. GEOPOLITYCZNE I GEOEKONOMICZNE ZNACZENIE TECHNOLOGII KOSMICZNYCH

Przestrzeń kosmiczna, a szczególnie orbita okołoziemska, stanowi obszar, który ma geopolityczne znaczenie dla rywalizacji mocarstw. Z tego powodu technologiczny wyścig zbrojeń jest w Kosmosie równie szybki, co na Ziemi. Potencjał kosmiczny państwa można mierzyć liczbą posiadanych satelitów i zdolnością do ich wynoszenia, nie mówiąc już o misjach załogowych czy międzyplanetarnych, które definiują wyższy poziom tych zdolności. W kręgach kosmicznych popularne jest powiedzenie: *space is hard*, którego źródłem jest historia zakończonych niepowodzeniem misji kosmicznych. Jeśli urządzenie za kilkaset milionów dolarów nie zaczyna działać na orbicie, trzeba wydać kolejne kilkaset milionów albo zmienić plany. Dlatego Kosmos skutecznie weryfikuje kulturę techniczną i zdolności organizacyjne państwa, a zakres planów jest użyteczną miarą krajowych zasobów gospodarczych.

Równowagę sił w kosmosie można określić przy pomocy kilku wskaźników takich jak:

- liczba wystrzelonych satelitów (państwa narodowe konkurują tu z ponadnarodowymi korporacjami),
- zdolność do wysyłania misji załogowych,
- zdolność do wysyłania misji księżycowych i międzyplanetarnych,
- posiadanie własnego kosmodromu (tu naturalną przewagę mają państwa leżące w pobliżu równika), posiadanie własnej technologii budowania satelitów i statków kosmicznych oraz technologii wynoszenia.

Należy zauważyć, że technologie kosmiczne ze swej natury są technologiami podwójnego zastosowania. Zdolność do budowy i wynoszenia satelitów i statków kosmicznych umożliwia potencjalnie również przenoszenie ładunków balistycznych. W wyścigu kosmicznym poza USA i Rosją partycypują także Chiny, Wielka Brytania, Japonia, Indie, a także niektóre kraje członkowskie UE, przede wszystkim Francja, Niemcy i Włochy. Poniższa grafika przedstawia ranking państw wedle liczby posiadanych satelitów.



Źródło: *2,062 space odysseys*, The Economist, [w:] *Attacking satellites is increasingly attractive and dangerous*, The Economist, 18.07.2019, [online:] https://www.economist.com/briefing/2019/07/18/attacking-satellites-is-increasingly-attractive-and-dangerous

Państwa, które prowadzą aktywną politykę kosmiczną, są zarazem producentami technologii kosmicznych, co pozwala im na dużą swobodę w definiowaniu celów, nie mówiąc już o zyskach, jakie wypracowuje narodowy przemysł kosmiczny. Skuteczne wyniesienie na orbitę okołoziemską satelity – zbudowanego przy użyciu własnych technologii i wyniesionego przy wykorzystaniu własnej rakiety nośnej – wiąże się z prestiżem międzynarodowym, gdyż oznacza dołączenie do wąskiego grona państw zdolnych do lotów kosmicznych (ang. *space-faring nations*). W tym kontekście kluczowe jest posiadanie właśnie zdolności autonomicznych, tj. opartych o posiadane technologie, przemysł i infrastrukturę. Doszły do tego chociażby Indie, w których budżet organizacji badań kosmicznych ISRO wynosi 1,3 mld USD[2] (dla porównania, budżet Polskiej Agencji Kosmicznej na 2019 r. wynosił 67 mln USD, a więc zaledwie 5% budżetu ISRO).

PRZESTRZEŃ KOSMICZNA JAKO POLE RYWALIZACJI MOCARSTW

Kosmos został zmilitaryzowany już na początku wyścigu kosmicznego: zbyt wiele możliwości oferował w zakresie obserwacji przeciwnika. Z czasów zimnej wojny datuje się także rozwój broni kosmicznej. Wydaje się, iż nikt nie zaryzykuje globalnego konfliktu kosmicznego, który mógłby mieć katastrofalne konsekwencje dla zdolności użytkowania orbity geostacjonarnej i uniemożliwić eksploatację przestrzeni okołoziemskiej na długie lata. Obecnie do interakcji mocarstw w kosmosie należą incydenty podobne do naruszania przez rosyjskie samoloty przestrzeni powietrznej NATO – w celu sprawdzenia czujności załóg programu *Air Policing*[3]. Polegają one na zbliżeniu na niewielką odległość do rakiety[4] lub satelity szpiegowskiego[5,6] w celu zbierania informacji, fotografowania oprzyrządowania lub prób zaburzania przesyłu informacji. Obszarem szczególnie istotnym jest obecnie cyberbezpieczeństwo systemów satelitarnych, zwłaszcza tych powstałych jeszcze w czasach, gdy cyberataki nie były postrzegane jako realne zagrożenie[7]. Przykład takiego cyberataku został omówiony na tegorocznej konferencji Black Hat[8] – ataki tego typu mają na celu przejęcie kontroli nad systemem, spowodowanie jego niedostępności lub też przechwycenie wysyłanych na Ziemię informacji.

Katastrofa Challengera doprowadziła w 2011 r. do zatrzymania amerykańskiego programu promów kosmicznych oraz, pośrednio, do zahamowania programu rozwoju wielostopniowych rakiet nośnych na dziewięć lat. USA utraciły wtedy czasowo możliwości wysyłania misji załogowych oraz samodzielnego zaopatrywania Międzynarodowej Stacji Kosmicznej (ISS)[9]. Skorzystała na tym Rosja, która dzięki temu utrzymała i rozwinęła produkcję silników rakietowych i rakiet Sojuz. Do czasu konfliktu rosyjsko-ukraińskiego w programie tym uczestniczyła także Ukraina, która dysponuje zakładami budowy silników rakietowych.

W roku 2019 Stany Zjednoczone powołały Siły Kosmiczne, co stanowi kontynuację deklaracji Sesji Rady Północnoatlantyckiej z 20 listopada 2019 r. o przyjęciu kosmosu jako piątej domeny prowadzenia operacji militarnych. Celem deklarowanym jest obrona satelitów przed bronią antysatelitarną czy też zakłóceniem lub hakowaniem ich pracy. Niszczenie satelitów na orbicie stanowi niewątpliwy *casus belli*, lecz poza tym stanowi broń obusieczną ze względu na syndrom Kesslera[10]: rozbicie satelity na fragmenty w wyniku kolizji zwiększa prawdopodobieństwo kolizji kolejnych satelitów z fragmentami, co powoduje efekt lawinowy. Może on zniszczyć wszystkie satelity na zbliżonych orbitach i zanieczyścić przestrzeń kosmiczną w sposób, który w praktyce wyeliminuje możliwości operacyjne technik satelitarnych na lata.

Przykładem niezależnego rozwoju technologii kosmicznych są Chiny, które od wielu lat rozwijały technologię wielostopniowych rakiet balistycznych w ramach wyścigu zbrojeń. W ominięciu amerykańskiego embargo na produkty wojskowe ITAR[a] pomogła Chińczykom europejska firma Thales Alenia Space, co z kolei wzmocniło jej

a International Traffic in Arms Regulation.

pozycję konkurencyjną w Europie względem rywala Airbusa[11]. Chińczycy zainwestowali również w europejski system nawigacji Galileo, który stanowi ważne uzupełnienie zbudowanego przez nich systemu Beidou. Przykładów współpracy europejsko-chińskiej jest więcej, np. w 2016 roku służby na całym świecie zaalarmowało wystrzelenie przez Chińczyków pierwszego satelity dostarczającego kluczy kryptograficznych za pomocą (prawie) niemożliwej do podsłuchania kryptografii kwantowej[12,13]. Technologia optyczna na pokładzie pochodziła z Austrii.

W kwestii telekomunikacji satelitarnej sytuacja zmienia się dynamicznie. Unia Europejska jest obok NATO jednym z aktywnych graczy, który stymuluje rozwój (w wybranym przez siebie kierunku) w naszej części świata. Potencjał Unii Europejskiej w dziedzinie badań najlepiej reprezentuje rozmiar i budżet powstałej w 1975 r. Europejskiej Agencji Kosmicznej, która zatrudnia 1900 osób przy budżecie 4 mld euro. Budżet NASA to 22 mld USD – to tylko cywilny komponent amerykańskiego programu: odrębne budżety na operacje kosmiczne ma Pentagon – 14,1 mld USD wg planu na 2020 – i NSA (budżet utajniony)[14]. Wspomniany już budżet indyjskiej agencji ISRO to 1,3 mld USD. Dla porównania Chiny wydały w 2017 r. 8,4 mld USD, zaś program rosyjski został obcięty do 3 mld USD.

Jedna z ważniejszych inicjatyw w zakresie telekomunikacji dotyczy sektora publicznego; mowa tu o unijnym programie GovSatCom[15]. Jego celem jest zapewnienie bezpiecznych usług telekomunikacyjnych dla administracji i agencji rządowych, służb ratowniczych, poszukiwawczych czy agencji unijnych takich jak FRONTEX. Komponent kosmiczny tego programu znajduje się obecnie na etapie pilotażowym[16], ambicje w tym obszarze deklaruje na przykład obecna również w Polsce luksemburska spółka SES[17]. Potrzeby w tym zakresie deklarują również polskie podmioty prywatne i państwowe[18]. Więcej na ten temat w dalszej części tekstu.

Unia Europejska, a konkretnie DG CONNECT, patronuje także ciekawemu przedsięwzięciu: EuroQCI, które jest na etapie studium wykonalności. Jest to inicjatywa integracji sieci narodowych kryptografii kwantowej (lub budowy tam, gdzie ich nie ma). Kryptografia kwantowa to, mówiąc w skrócie, propozycja użycia dedykowanych łącz optycznych, naziemnych lub satelitarnych do dystrybucji kluczy kryptograficznych, które umożliwiają bezpieczne połączenia. W procesie rozwoju tej technologii są, poza inicjatywą UE, różne wektory; wspomniany był przykład Austrii, która uczestniczyła w chińskim programie budowy takiego satelity, zaś pierwsza poza kontynentalnymi Chinami transmisja szyfrowana za pomocą klucza kwantowego nastąpiła pomiędzy Pekinem a Wiedniem. Systemy takie jak EuroQCI powstają również w USA i innych krajach.

W kontekście Europy nie sposób nie wspomnieć Europejskiej Agencji Kosmicznej (European Space Aagency – ESA). W wielu aktywnościach ESA biorą udział, co zrozumiałe, silni producenci technologii kosmicznych, tacy jak Airbus czy Thales Alenia Space, którzy często zostają interesariuszami oraz realizatorami, a w konsekwencji beneficjentami projektów ESA. Temu zjawisku trudno się dziwić: europejskie mocarstwa kosmiczne, Francja, Niemcy i Włochy, pokrywają 60,7% budżetu ESA (wg danych na 2020). ESA definiuje swoją misję jako platformy i promotora porozumienia między państwami europejskimi w zakresie badań i rozwoju technologii kosmicznych oraz ich zastosowań, z intencją ich użycia do celów naukowych oraz do celu zastosowań operacyjnych[19]. Największymi beneficjentami ESA są państwa, które posiadają własną technologię kosmiczną. Jest to zrozumiałe ze względu na model działania ESA, która ułatwia rozwój technologii, a kiedy ta osiągnie dojrzałość, korzystają z niej przede wszystkim europejscy giganci przemysłu kosmicznego. Ważnymi graczami w wyścigu kosmicznym są jednak nie tylko państwa narodowe i przedsiębiorstwa państwowe, ale także podmioty sektora prywatnego, które wchodzą w obszary dotąd dla nich niedostępne. Znaczącym punktem w czasie jest rok 2020, w którym po raz pierwszy prywatna firma wyniosła astronautów na pokład ISS, co zakończyło dekadę względnej

równowagi między USA i Rosją, ale zarazem wprowadziła do geopolityki kosmicznej nowego gracza w postaci Elona Muska, który reprezentuje korporację, a nie państwo narodowe[20]. **Kosmos, który za sprawą ogromnych kosztów eksploracji był dotąd domeną państw narodowych i organizacji międzynarodowych takich jak ESA (Europejska Agencja Kosmiczna), przechodzi w ręce multikorporacji, które rozpoczynają bezpardonowy wyścig zajmowania zasobów kosmicznych. Zapowiedź Elona Muska o wystrzeleniu 12 000 satelitów megakonstelacji Starlink, które mają dostarczyć każdemu Ziemianinowi satelitarny internet, może zachwiać dotychczasową równowagą sił**[21].

POZYCJA I POTENCJAŁ TRÓJMORZA W TYM REKOMENDACJE DLA POLSKI

Na kraje Trójmorza przypada dziś jedynie 14 satelitów z ogólnej liczby 2667, w tym 11 satelitów to projekty studenckie, testy technologii lub obserwacja kosmosu czy ziemskiego pola elektromagnetycznego, a jedynie 3 można uznać – również nie bez zastrzeżeń – za projekty komercyjne o wymiernym potencjale gospodarczym[22]. Wszystkie satelity z tej liczby zajmują niskie orbity okołoziemskie (LEO), co oznacza, że żadne z państw Trójmorza nie wykorzystuje bezpośrednio i samodzielnie przyznanego mu miejsca na orbicie geostacjonarnej. Zgodnie z danymi World Teleport Association na obszarze Trójmorza niezależne, komercyjne komponenty naziemne telekomunikacji satelitarnej (tzw. teleporty), które są zrzeszone w ramach organizacji, posiadają tylko Austria, Węgry, Słowenia i Bułgaria, choć oczywiście anten nadawczych i niezrzeszonych teleportów (na przykład Antenna Hungaria) jest więcej. **Warto podjąć inicjatywę strategiczną przeglądu teleportów z obszaru Trójmorza i podzielić podmioty na prywatne, które znajdują się pod całkowitą lub częściową kontrolą państwową, co określi możliwy zakres ich użycia.** Telekomunikacja satelitarna daje alternatywę dla światłowodu i jest uzupełnieniem takich inicjatyw jak 3 Seas Digital Highway. **Strategicznym kierunkiem prac w zakresie budowania wizerunku Trójmorza powinna być także umiejętna polityka kadrowa polegająca na popieraniu kandydatów z krajów 3SI w strukturach ESA.** Od krajów Trójmorza pochodzi wprawdzie tylko 3% budżetu ESA na 2020 rok[23], jednak z drugiej strony obszar ten reprezentuje 15% populacji Europy i podobny potencjał w zakresie rozmiarów rynku dla usług satelitarnych. Rosnąca rola Trójmorza przejawia się m.in. w budowie w 2004 r. w Pradze centrum utrzymania europejskiego systemu nawigacyjnego GNSS, którego misja ma objąć m.in. o budowę pozycji rynkowej tego systemu (konkurs „Twój dron z GNSS") czy zagadnienia bezpieczeństwa[24]. W tym zakresie dla rozwoju całego regionu istotne jest nawiązanie współpracy z rządem Czech w ramach inicjatywy Trójmorza. Ciekawą inicjatywą, z której skorzystały dotąd Estonia i Węgry, jest możliwość uruchomienia inkubatorów biznesu kosmicznego[25] pod patronatem ESA. **Istotnym elementem geostrategicznego rozwoju regionu jest rozpoznanie poglądów państw Trójmorza w tym zakresie i rozważenie koordynacji budowania polityki kosmicznej.** Przykładem jest tu NATO, który prowadzi wspólną politykę, ale realizuje ją za pośrednictwem inicjatyw państw narodowych.

POZYCJA POLSKI W WYŚCIGU KOSMICZNYM

Po akcesji do Unii Europejskiej i NATO Polska uzyskała dostęp do zasobów satelitarnych do obserwacji Ziemi. Mimo to wciąż brak jej autonomicznych zdolności w tym zakresie. W obszarze technologii obrazowania satelitarnego nie ma ani jednej polskiej firmy prywatnej, spółki kontrolowanej przez Skarb Państwa ani podmiotu państwowego (wliczając siły zbrojne), który w sposób całkowicie autonomiczny mogłaby dokonywać zobrazowań dla celów cywilnych i militarnych. Ponieważ rynek polski jest całkowicie zależny od zagranicznych dostawców, mają oni jednocześnie kompletny wgląd w potrzeby Polski w zakresie zobrazowań. Zobrazowania są zamawiane przez każdą jednostkę oddzielnie, zgodnie z procedurą przetargową, w związku z tym wykonawca przetargu ma wgląd w zapotrzebowanie danej jednostki na zobrazowania. Daje to ogromne możliwości pozyskiwania informacji dla obcych wywiadów: gospodarczego, cywilnego i wojskowego.

Chwalebny jest udział polskich firm jako wykonawców elementów wykorzystywanych w projektach Europejskiej Agencji Kosmicznej – zdarza się zresztą, że skutecznie konkurują one z europejskimi liderami tego sektora. Tym niemniej Polska nie posiada dużego przemysłu satelitarnego i w związku z tym nie ma wpływu na decyzje ESA, zaś interesariuszami i odbiorcami technologii satelitarnych rozwijanych przez ESA są najwięksi gracze europejskiego rynku kosmicznego.

Ambicją Polski, według deklaracji Ministerstwa Gospodarki i zgodnie z Polską Strategią Komiczną, jest osiągnięcie przez polskie przedsiębiorstwa 3% udziału w obrotach europejskiego rynku kosmicznego. Spotyka się głosy, że do spełnienia tego warunku wystarczy podnieść naszą składkę do ESA[b]. **Jeśli jednak Polska nie podejmie inicjatywy w zakresie samodzielnego definiowania celów dla autonomicznego rozwoju gospodarki ze strony administracji publicznej lub spółek skarbu państwa, nie zbuduje trwałych zdolności kosmicznych.** Wato przypomnieć, że amerykański program Apollo, który był kołem zamachowym amerykańskiej gospodarki i przekształcił zimnowojenną rywalizację geopolityczną między USA i ZSRR, powstał w drodze inwestycji dokonanej przez amerykańską agencję rządową[c]. Działania, w których państwo jest głównym inicjatorem rozwoju przemysłu kosmicznego, nie muszą stać w sprzeczności z interesem rynku kosmicznego. Administracja państwowa będzie preferencyjnie zamawiać te usługi, w których powstanie sama zainwestowała. Biorąc na wzgląd polskie ambicje, celowe wydaje się wzmocnienie, poczynając od poziomu aktów prawnych i dokumentów koncepcyjnych, roli państwa jako koła napędowego polskiej polityki kosmicznej i śmiałe zdefiniowanie celów tej polityki z pomocą posiadanych przez państwo aktywów i instrumentów inwestycyjnych. W modelu rozwoju takich państw jak USA, Chiny, Indie czy Rosja występuje duży poziom zaangażowania budżetu państwa, który w konsekwencji umożliwia rozwój przemysłu i generowanie zysków.

Krajowy program dotyczący sektora kosmicznego zmierzający do uzyskania autonomicznych możliwości w zakresie obrazowania był już celem prac przygotowawczych, zamówionych m.in. przez NCBiR, a także przedmiotem studium wykonalności, sporządzonego przez konsorcjum pod przewodem Wojskowej Akademii Technicznej już w 2015 r., a więc 43 lata po wystrzeleniu pierwszego na świecie satelity obserwacyjnego. Paradoksalnie Polska może jeszcze zyskać na stosunkowo późnym uruchomieniu swojej polityki kosmicznej, ponieważ w międzyczasie rozpoczęła się dyskusja nad celowością dalszej budowy dużych satelitów – o masie powyżej 0,5 tony – i znacząco rozwinął się rynek nanosatelitów. Redukcja masy związana jest z innowacjami w zakresie technologii: układy optyczne, które kiedyś były realizowane we wnętrzu satelity obserwacyjnego o dużej masie, można dziś budować w technologiach rozkładanych modułów optycznych. Te innowacyjne technologie (także w odniesieniu do technologii obrazowania radarowego SAR czy optoelektroniki) rozwijane są także przez polskie firmy[26]. Warto też odnotować, że potencjał i doświadczenie polskich ekspertów w zakresie cyberbezpieczeństwa ma także swój kontekst kosmiczny. Mimo znikomego *space heritage* polskiego przemysłu potrafią oni wygrywać w międzynarodowych konkursach (konkurs Hack-A-Sat zorganizowany w 2020 przez Siły Powietrzne Stanów Zjednoczonych[27]) poświęconych bezpieczeństwu technologii satelitarnych. Mimo że w Polsce nie rozwija się przecież szeroko tych technologii i wiele z zagadnień było

b Spotyka się opinie, że realizacja tego celu jest prosta: wystarczy odpowiednio podnieść składkę do ESA – źródło: Ziemnicki P., *Kosmos na Kongresie 590. Administracja powinna być pierwszym klientem sektora [RELACJA]*, Space24, 16.11.2019, [online:] https://www.space24.pl/kosmos-na-kongresie-590-administracja-powinna-byc-pierwszym-klientem-sektora-relacja.

c Nie wspominając o takich drobiazgach jak Internet, w który inwestowała DARPA, lądowanie na Księżycu, półprzewodniki czy sztuczna inteligencja. Źródło: *DARPA 60 Years 1958-2018*, DARPA, 2018, [online:] https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf.

dla naszych inżynierów pewną nowością, zespół Poland Can Into Space zajął w punktacji generalnej drugie miejsce[28]. Również w obszarze łącz optycznych Polska może wykorzystać potencjał polskiego przemysłu optoelektronicznego.

Tym niemniej należy pamiętać, że dla **przedsiębiorstwa czy instytucji naukowej, które nie realizowały jeszcze technologii czy badań kosmicznych, wejście na rynek europejski jest trudne. Program narodowy stanowi dla takich jednostek naturalną szansę na zebranie doświadczenia kosmicznego (tzw. *space heritage*).**

Premier Mateusz Morawiecki, potwierdzając ambicje Polski w zakresie budowy polskiego satelity, podkreślił wagę inicjatyw ze strony przedsiębiorstw[29], w tym kierunku idzie również rozstrzygnięty niedawno konkurs NCBiR na projekty szybkiej ścieżki „Technologie kosmiczne"[d]. Program taki jest wzmiankowany w Polskiej Strategii Kosmicznej. Warto jednak zauważyć, że ani Cele Strategiczne, ani Cele Szczegółowe nie stwierdzają jednoznacznie, że drogą do pozyskania własnych zobrazowań przez krajowe przedsiębiorstwa ma być rozwój własnego satelity. Cele Szczegółowe mówią o rozwoju aplikacji satelitarnych oraz o rozbudowie zdolności, nie wyróżniając priorytetowej roli polskiego programu budowy własnego satelity, który ma ważną misję uniezależnienia w zakresie pozyskiwania zobrazowań od rynków zagranicznych. Troski o autonomię wymaga również rynek telekomunikacji satelitarnej.

REKOMENDACJE DLA POLSKI

Podstawowym priorytetem dla Polski jest podjęcie działań koniecznych dla wystrzelenia własnego satelity lub konstelacji satelitów, świadczących usługi w zakresie obrazowania dla polskich podmiotów i zapewnienie długofalowego finansowania tego projektu[30].

Kolejne istotne zagadnienie dotyczy własności przedsiębiorstw polskiego sektora satelitarnego. Przedsiębiorstwa tego sektora, nierzadko specjalizujące się w wysokich technologiach i w przeszłości doinwestowane przez Państwo w ramach różnych programów rozwojowych, stanowią prawie w 100% wartość prywatną. Są to zarazem jednostki z sektora MŚP o stosunkowo niewielkiej kapitalizacji, co zwiększa ich mobilność i zdolność do prowadzenia agresywnej polityki rozwoju i innowacji, ale jednocześnie czyni je wrażliwymi na próby przejęcia. Pewnym wyjątkiem jest 19,35% akcji Creotech, które nabyła Agencja Rozwoju Przemysłu S.A.[31]. Polski rynek jest rozdrobniony. Niewątpliwe kompetencje polskich inżynierów są rozproszone po małych firmach, które często konkurują o granty z tych samych programów grantowych, a po uruchomieniu produkcyjnym swoich usług będą konkurować między sobą (i ze światowymi gigantami) o polski rynek obrazowania. **Celowe wydaje się działanie na rzecz regulacji rynku zobrazowań, choćby w celu redukcji kosztów ponoszonych zobrazowań i uwspólnianie zamówień. Drugi kierunek to działania koordynacyjne takie jak utworzenie klastra kosmicznego[e] i inwestycje kapitałowe za pośrednictwem Spółek Skarbu Państwa czy Polskiego Funduszu Rozwoju w celu realizacji polskiej strategii kosmicznej: czy to celowe, w Spółkach Skarbu Państwa, czy też w wyróżniających się start-upach, w celu konsolidacji rynku. Większym organizacjom łatwiej jest ponosić ryzyko inwestycyjne czy inwestować w przygotowanie oferty przetargowej. Ambicje polskich wizjonerów rynku kosmicznego warto zmienić na współdziałanie: kto by miał wątpliwości w tej sprawie, niech prześledzi historię biznesową Airbusa[f], która wskazuje, że konsolidacja generalnie się opłaca.**

Przystąpienie Polski do programu GovSatCom jest rekomendowane jako jeden z celów Polskiej Strategii Kosmicznej, zaś środowiska zbliżone do ESA, SES i POLSA prowadzą w tej sprawie działania informacyjne[32]. **Przystąpienie do GovSatCom jest możliwością do rozważenia, z uwagi na redukcję kosztów utrzymania infrastruktury telekomunikacyjnej. Jednak potrzebna jest pogłębiona analiza potrzeb Polski, wszystkich interesariuszy instytucjonalnych i specjalistów w dziedzinie analizy ryzyka, z uwzględnieniem potrzeb i potencjału Trójmorza, która powinna poprzedzać tak strategiczną decyzję technologiczną.** Każde przystąpienie do wspólnego programu stanowi ograniczenie wykonywania przez państwo niektórych kompetencji, w tym przypadku – możliwości wyboru celów rozwoju i wyboru technologii i partnerów technologicznych. Wiążą się również z dalszym otwarciem rynku na rzecz międzynarodowego operatora telekomunikacyjnego (operatora wspólnej, europejskiej usługi). **Przystąpienie do programu GovSatCom nie umniejsza potencjalnej wagi posiadania polskiego satelity telekomunikacyjnego. Potrzeba jego opracowania może być jednym z wniosków wspomnianej wyżej analizy.**

Pozytywną zmianą jest rosnąca aktywność polskich firm na rynku satelitarnym takich jak SatRevolution, Creotech, Scanway, Thorium czy EXATEL, a także wielu firm zagranicznych działających na obszarze Polski, w których zatrudnienie znajdują polscy inżynierowie branży kosmicznej. **Państwo polskie powinno być aktywnym graczem na tym rynku, i to takim, który stawia firmom wyżej poprzeczkę technologiczną i daje stabilne warunki długofalowego finansowania.**

d Gwoli kronikarskiej ścisłości, warto wspomnieć, że całkowity budżet programu, a więc 311 milionów PLN pokrywa ok. 50% kosztów wystrzelenia komercyjnego satelity.

e Postulat takiego działania jest silnie wspierany przez m.in. EXATEL, którego autor jest pracownikiem.

f U jej zarania pojawia się kilka nazw przedsiębiorstw znanych na przykład z książki Arkadego Fiedlera.

PRZYPISY

1 *Orbiter STS*, Wikipedia, 12.09.2020, https://pl.wikipedia.org/wiki/Orbiter_STS

2 *Indyjska Organizacja Badań Kosmicznych*, Wikipedia, 12.09.2020, [online:] https://pl.wikipedia.org/wiki/Indyjska_Organizacja_Bada%C5%84_Kosmicznych

3 *Allied fighter jets intercept Russian aircraft*, NATO, 12.09.2020, [online:] https://www.nato.int/cps/en/natohq/news_174349.htm?selectedLocale=en.

4 Gruss M., *Maneuvering Russian Satellite Has Everyone's Attention*, Space News, 12.09.2020, [online:] https://spacenews.com/maneuvering-russian-satellite-has-everyones-attention/

5 Hennigan W. J., *Exclusive: Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says*, Time, 12.09.2020, [online:] https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/

6 Weeden B., *Dancing in the dark redux: Recent Russian rendezvous and proximity operations in space*, The Space Review, 12.09.2020, [online:] https://www.thespacereview.com/article/2839/2.

7 Whitwam R., *Hacking Satellites Is Surprisingly Simple*, ExtremeTech, 12.09.2020, [online:] https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think

8 Palmer D., *How hackers could spy on satellite internet traffic with just $300 of home TV equipment*, ZDNet, 12.09.2020, [online:] https://www.zdnet.com/article/how-hackers-could-spy-on-satellite-internet-traffic-with-just-300-of-home-tv-equipment/

9 Goetz E., *The impact of the crisis in Ukraine on the effort to reform U.S. space controls*, WorldECR, 12.09.2020, [online:] https://www.crowell.com/files/the-impact-of-the-crisis-in-ukraine-on-the-effort-to-reform-u.s.-space-controls.pdf.

10 Wikipedia, 12.09.2020, [online:] https://en.wikipedia.org/wiki/Kessler_syndrome.

11 https://www.aei.org/articles/chinas-space-ambitions/, dostęp 12.09.2020

12 Castelvecchi D., *China's quantum satellite clears major hurdle on way to ultrasecure communications*, Nature, 12.09.2020, [online:] https://www.nature.com/news/china-s-quantum-satellite-clears-major-hurdle-on-way-to-ultrasecure-communications-1.22142.

13 Tamże.

14 Erwin S., *Military space gets big boost in Pentagon's $750 billion budget plan*, SpaceNews, 12.09.2020, [online:] https://spacenews.com/militaryspace-gets-big-boost-in-pentagons-750-billio/.

15 Borek R., Hopej K., Chodosiewicz P., *GOVSATCOM makes EU stronger on security and defence*, Security and Defence Quarterly 28 no. 1, 2020, s. 44–53.

16 *Govsatcom Precursor for security*, The European Space Agency, 31.08.2020, [online:] https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Govsatcom_Precursor_for_security.

17 *GOVSATCOM DEMO SESSIONS*, SES, 31.08.2020, [online:] https://www.ses.com/govsatcom-demo-sessions.

18 *W oczekiwaniu na GovSatCom. Wyniki ankiety PAK dotyczącej łączności satelitarnej*, Space24, 31.08.2020, [online:] https://www.space24.pl/w-oczekiwaniu-na-govsatcom-wyniki-ankiety-pak-dotyczacej-lacznosci-satelitarnej.

19 *ESA's Purpose*, The European Space Agency, 31.08.2020, [online:] https://www.esa.int/About_Us/Corporate_news/ESA_s_Purpose

20 Crane L., *SpaceX to make history launching NASA astronauts on a private rocket*, NewScientist, 12.09.2020, [online:] https://www.newscientist.com/article/2244541-spacex-to-make-history-launching-nasa-astronauts-on-a-private-rocket/.

21 *Starlink*, Wikipedia, 12.08.2020, [online:] https://en.wikipedia.org/wiki/Starlink.

22 Wg UCS Satellite Database, 29.08.2020, [online:] https://www.ucsusa.org/resources/satellite-database.

23 *ESA Budget 2020*, The European Space Agency, 31.08.2020, [online:] https://www.esa.int/ESA_Multimedia/Images/2020/01/ESA_budget_2020.

24 *Questions and Answers on the new EU Space Programme*, European Commission, 31.08.2020, [online:] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4023.

25 *ESA Business Incubation Centers*, The European Space Agency, 31.08.2020, [online:] http://www.esa.int/Applications/Telecommunications_Integrated_Applications/Business_Incubation/ESA_Business_Incubation_Centres23.

26 *WROCŁAWSKI STARTUP, SATREVOLUTION, WYRUSZA NA PODBÓJ KOSMOSU*, Outsourcing Portal, 29.08.2020, [online:] http://www.outsourcingportal.eu/pl/wroclawski-startup-satrevolution-wyrusza-na-podboj-kosmosu.

27 *Hackasat, czyli konkurs hakowania satelity*, Astroblog, 29.08.2020, [online:] https://www.astroblog.aroch.pl/wydarzenia/hackasat-czyli-konkurs-hakowania-satelity/.

28 Hackasat, Twitter, 29.08.2020, [online:] https://twitter.com/p4_team/status/1292240067742838790, https://www.hackasat.com/.

29 *Morawiecki: budowa satelity polską ambicją*, Space24, 29.08.2020, [online:] https://www.space24.pl/wiadomosci/morawiecki-budowa-satelity-polska-ambicja.

30 Ziemnicki P., *Kosmos na Kongresie 590. Administracja powinna być pierwszym klientem sektora [RELACJA]*, Space24, 16.11.2019, [online:] https://www.space24.pl/kosmos-na-kongresie-590-administracja-powinna-byc-pierwszym-klientem-sektora-relacja

31 29.08.2020, [online:] https://www.arp.pl/o-arp/spolki-w-nadzorze-wlascicielskim-arp.

32 Borek R., Hopej K., Chodosiewicz P., *GOVSATCOM makes EU stronger on security and defence*, op. cit.

Dr Joanna Świątkowska

OFENSYWNE DZIAŁANIA W CYBERPRZESTRZENI – CZYNNIK KSZTAŁTUJĄCY GEOPOLITYKĘ

W 2017 roku szefowie agencji wywiadowczych USA we wspólnym oświadczeniu przed Komisją Sił Zbrojnych Senatu Stanów Zjednoczonych stwierdzili, że więcej niż trzydzieści państw rozwija zdolności do przeprowadzania ofensywnych działań w cyberprzestrzeni. Liczba ta, choć prawdopodobnie niższa niż w rzeczywistości, wskazuje trend, który nie może dziwić. Dzisiaj jest już wiedzą oczywistą, że cyfrowe zdolności stanowią ważny element bezpieczeństwa i potęgi współczesnych państw. Nie ulega wątpliwości, że ofensywne działania prowadzone w cyberprzestrzeni mogą służyć projekcji siły oraz być ważnym elementem służącym osłabieniu rywala.

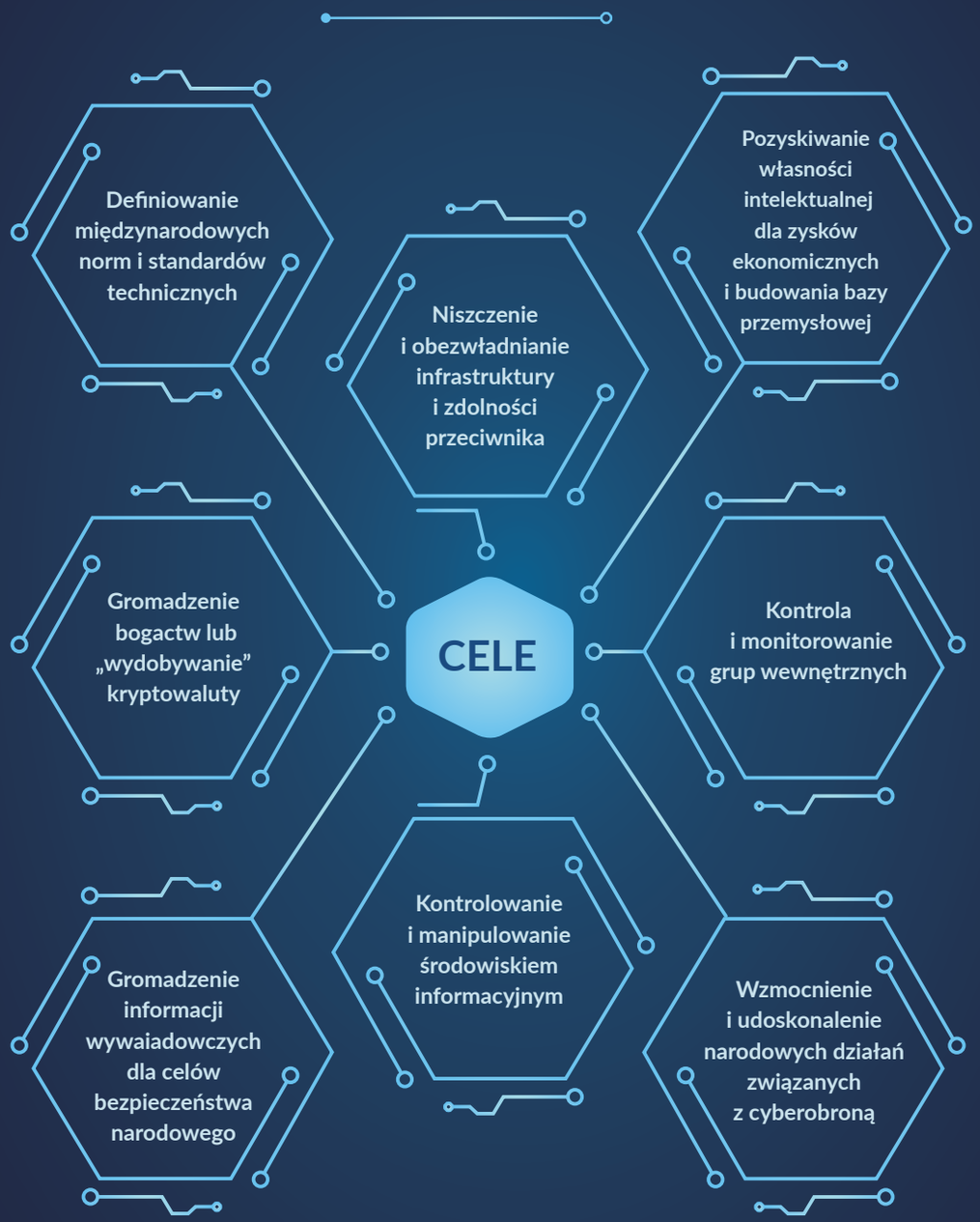
Zespół badaczy z Belfer Center for Science and International Affairs wyróżnił osiem strategicznych celów ważnych z punktu widzenia budowania potęgi, które podmioty państwowe próbują osiągnąć, wykorzystując narzędzia cyfrowe (patrz rys. 1). Lista wyraźnie pokazuje, że w większości przypadków do ich realizacji konieczne będzie przynajmniej posiadanie możliwości skorzystania z technik ofensywnych.

OFENSYWNE DZIAŁANIA – CZYM SĄ I DO CZEGO PROWADZĄ?

Jednym z problemów w dyskusji nad ofensywnymi działaniami w cyberprzestrzeni jest trudność w określeniu ich definicji, a nawet funkcji. Można przyjąć, że ofensywne operacje w cyberprzestrzeni to działania podejmowane z użyciem środków cyfrowych, których celem jest manipulacja, zniszczenie lub zakłócenie funkcjonowania systemów

RYSUNEK 1

CELE PAŃSTW REALIZOWANE PRZY UŻYCIU ŚRODKÓW CYFROWYCH



Źródło: Voo J. et al., *Reconceptualizing Cyber Power, Cyber Power Index Primer.* Belfer Center for Science and International Affairs, Cambridge, 2020

i sieci teleinformatycznych i przetwarzanych za ich pomocą danych[1]. Często doktryna wojskowa, jak również poszczególni badacze[a] odrębnie traktują działania wywiadowcze prowadzone w cyberprzestrzeni[b]. Służą one rozpoznaniu systemów przeciwnika, pozyskaniu danych i informacji, nie dokonaniu zniszczeń czy szkód. Tutaj jednak cyberszpiegostwo będzie uznawane za podkategorie działań ofensywnych skupiających się na ingerencji w systemy przeciwnika.

Do pewnego czasu, przede wszystkim wśród państw Zachodu, dominowało rozumienie cyberzagrożeń przez pryzmat głównie technologiczny. W centrum obrony znajdowały się komputery, dane, systemy. Tymczasem z biegiem czasu stało się jasne, że cyberprzestrzeń może być wykorzystywana do wrogich działań, których głównym celem nie są maszyny, funkcje przez nich realizowane, ale człowiek – jego percepcja, decyzje i działania. Dezinformacja, manipulacja, propaganda – wybory prezydenckie w USA z 2016 roku i w ostatnim czasie pandemia COVID-19 jasno pokazały, jaką siłę daje Internet we wpływaniu ludzi[c].

Państwa narażone są na wiele rodzajów ofensywnych działań prowadzonych w sieci. Stać za nimi mogą różne podmioty, mające rozmaitą motywację do prowadzenia wrogich działań. Grupy przestępcze, pojedynczy kryminaliści, haktywiści czy grupy terrorystyczne wykorzystują sieć do osiągania swoich celów. Jednak przedmiotem tego artykułu będą ofensywne działania, które prowadzone są przez podmioty państwowe[d]. Są to najbardziej wyrafinowane, zaawansowane działania motywowane politycznie, a przez to wpływające na geopolitykę.

Ofensywne działania prowadzone w cyberprzestrzeni, za którymi stoją podmioty państwowe, nigdy nie są celem samym w sobie. Są działaniami wspierającymi, pozwalającymi realizować szersze interesy, najczęściej właśnie o charakterze politycznym, ekonomicznym, wojskowym etc. Mogą być prowadzone zarówno poniżej progu wojny, jak również stanowić istotny element działań zbrojnych. Wiąże się to ze zmianą doktryn militarnych oraz strategii, zmianami organizacyjnymi i ogólnie modyfikacją myślenia o naturze konfliktów.

Ostatnie lata przyniosły bardzo wiele przykładów ofensywnych działań prowadzonych w cyberprzestrzeni. Najgłośniejszym i najszerzej opisywanym był atak wirusa Stuxnet. Zainfekował on systemy irańskiej elektrowni atomowej i doprowadził do fizycznych zniszczeń wirówek służących do wzbogacania uranu, opóźniając w ten sposób program atomowy tego kraju. Była to jedna z bardziej wyrafinowanych i zaawansowanych operacji, najpewniej przeprowadzona przez USA oraz Izrael, która pokazała strategiczną wartość działań prowadzonych w sieci. Stuxnet był przykładem ataku prewencyjnego, ale jak wskazują Max Smeets i Herbert S. Lin, powołując się na doniesienia „The New York Times", USA miały w zanadrzu plan jeszcze bardziej rozległej, wyprzedzającej operacji ofensywnej znanej jako Nitro Zeus[2]. Miała ona za zadanie doprowadzić do zniszczenia systemu ochrony przeciwpowietrznej Iranu, systemów komunikacyjnych tego kraju, jak również części sektora energetycznego. Stuxnet z racji swoich konsekwencji, politycznej motywacji i stopnia zaawansowania zmienił myślenie o zapewnianiu cyberbezpieczeństwa i roli ofensywnych działań prowadzonych w cyberprzestrzeni.

Cyberprzestrzeń jest dziś ściśle połączona z całym obszarem bezpieczeństwa narodowego. **Systemy i sieci teleinformatyczne stały się m.in. nieodłącznym elementem współczesnego pola walki, fundamentem funkcjonowania infrastruktury**

a Np. Smeets M., Lin H. S., *Offensive Cyber Capabilities: To What Ends?*, wyżej wspomniani badacze z ASPI, doktryna amerykańska: [online:] https://www.hsdl.org/?abstract&did=734860.

b W artykule używana będzie nazwa cyberszpiegostwo (choć jest to pewne uproszczenie).

c Owszem, w domenie wojskowej zwracano uwagę na możliwość eksploatacji cyberprzestrzeni do prowadzenia operacji psychologicznych, ale uważano, że działanie to realizowane będzie wyłącznie w okresie działań zbrojnych.

d Lub przez podmioty państwowe wspierane.

krytycznej, także cywilnej. Nie może zatem dziwić, że cyberataki stały się elementem towarzyszącym konfliktom. W grudniu 2015 roku w skoordynowany sposób zaatakowany został system energetyczny Ukrainy. W jego wyniku od prądu odciętych zostało około 100 miejscowości. Zarówno przedstawiciele władz Ukrainy, jak i rządu USA obarczyli winą za atak Rosję[3]. Atak przeprowadzony został równolegle do trwających na wschodzie Ukrainy walk zbrojnych z Rosją. Operację interpretować można jako próbę destabilizacji Ukrainy w środku konfliktu zbrojnego, obniżenia morale społeczeństwa, jak również manifestację siły agresora.

Rolę i znaczenie dostępu do sieci ilustruje także aktualna sytuacja na Białorusi, gdzie blokowanie Internetu stało się strategią reżimu obliczoną na osłabienie działań protestujących.

Cyberataki mające na celu destrukcję czy obniżanie zdolności podmiotów do realizowania ich funkcji to jedna z form ofensywnej działalności. Inną są wspomniane wcześniej działania wywiadowcze. Cyberszpiegostwo prowadzone w sieci jest działaniem powszechnie praktykowanym i o ile pozyskiwanie informacji o strategicznym znaczeniu znajduje milczące przyzwolenie graczy międzynarodowych, tak w ostatnich latach prawdziwą plagą wzbudzającą sprzeciw jest szpiegostwo przemysłowe przynoszące korzyści finansowe, niejednokrotnie wspierane lub bezpośrednio realizowane przez podmioty państwowe.

Jednym z najczęściej oskarżanych o kradzież własności intelektualnej i przemysłowej państwem są Chiny. Oskarżenia te wysuwały nie tylko USA, ale także inne kraje jak UK[4]. Chiny wedle tych doniesień mają parać się nielegalnym transferem wiedzy, danych i technologii, które pozwalają im budować innowacyjność, wspierać chińskie przedsiębiorstwa tanim kosztem i kosztem innych. W ten sposób państwo to buduje swoją pozycję w globalnym technologicznym wyścigu. Przykładem spektakularnej kampanii cyberszpiegowskiej, o którą oskarżane były Chiny, jest choćby kradzież projektów amerykańskiego myśliwca F-35[5]. Aktywne działania Chin w cyberprzestrzeni są jednym z powodów, dla których USA wraz z wieloma innymi krajami tak silnie sprzeciwia się budowaniu sieci 5G przez chińskie przedsiębiorstwa.

Z faktu coraz bardziej intensywnego wykorzystywania cyberprzestrzeni do prowadzenia działań ofensywnych wynika wiele wyzwań i implikacji dla międzynarodowego środowiska bezpieczeństwa i geopolityki. Wybrane z nich przedstawione zostały poniżej.

ATRYBUCJA I WYCIĄGANIE KONSEKWENCJI

Pierwszym wyzwaniem, które związane jest ze środowiskiem cyberprzestrzeni, jest trudność z ustalaniem odpowiedzialności za ataki. Jest to tak zwany problem atrybucji. Ponieważ ślady cyfrowe łatwo zmylić, zmanipulować, nie jest prostym zadaniem ustalenie i udowodnienie tego, kto faktycznie ponosi winę za dany atak. Łatwo zatem popełnić błąd, wysunąć fałszywe oskarżenia, doprowadzić do eskalacji konfliktu. Sprawca zyskuje także możliwość wyparcia się swojej odpowiedzialności przez powołanie się na niewystarczające dowody. Może także przerzucić winę na inne podmioty. Atrybucja jest więc zadaniem skomplikowanym, które wymaga połączenia informacji i dowodów z wielu domen. Informatyka śledcza, wiedza wywiadowcza, geopolityczny kontekst – wszystko powinno być brane pod uwagę. Pomimo że niełatwa, atrybucja jest pierwszym i niezbędnym krokiem do wyciągnięcia konsekwencji, ukarania sprawcy i doprowadzenia do potencjalnej zmiany jego zachowania. Poszczególni aktorzy coraz lepiej radzą sobie z tym wyzwaniem, co prowadzi do tego, że państwa i organizacje międzynarodowe coraz częściej decydują się na publiczne wskazanie winnych danych ataków[e]. Wciąż nieczęsto jednak atrybucji

e Przykładem publicznej atrybucji było m.in.: oskarżenie rosyjskich podmiotów o przeprowadzenie cyberataków na Gruzję w 2018 roku (atrybucji dokonały m.in. USA, Wielka Brytania, Gruzja, UE); oskarżenie Korei Północnej o dokonanie ataku „WannaCry" (atrybucja dokonana przede wszystkim przez USA); oskarżenie podmiotów rosyjskich o cyberatak na Organizację ds. Zakazu Broni Chemicznej (atrybucja dokonana m.in. przez Holandię, Wielką Brytanię oraz USA), oskarżenie rosyjskich podmiotów o przeprowadzenie ataku „NotPetya" (atrybucja dokonana przez Kanadę, USA, kilka państw europejskich).

tej towarzyszą konkretne odpowiedzi, na przykład w postaci sankcji. Państwem, które kilkukrotnie zdecydowały się na ten ruch, są USA. Prezydent Barack Obama zastosował ten mechanizm pierwszy raz w 2015 roku, nakładając sankcje na Koreę Północną w ramach odpowiedzi na cyberatak nakierowany na firmę Sony Pictures. Podobny los spotkał kilka podmiotów rosyjskich, które ukarane zostały za ingerencję w wybory prezydenckie w USA[6]. Unia Europejska także ustanowiła reżim sankcyjny, który może zostać użyty w odpowiedzi na ofensywne działania prowadzone w sieci Przez dłuższy czas mechanizmy te nie były aktywowane, co spotykało się z krytyką tych, którzy nawoływali do bardziej zdecydowanych działań. W sytuacji różnej percepcji państw członkowskich dotyczącej zagrożeń, analizowania potencjalnych działań w szerszym kontekście relacji międzynarodowych oraz zróżnicowanych interesów narodowych osiągnięcie wspólnego politycznego frontu jest zadaniem trudnym. Tymczasem w lipcu 2020 roku doszło do przełomu i UE po raz pierwszy w historii nałożyła sankcje na 6 osób i 3 podmioty powiązane z cyberatakami (próba cyberataku na OPCW; „WannaCry", „NotPetya" oraz „Operation Cloud Hopper").

Przejście od słów do czynów jest bardzo istotne, bowiem bezczynność i wyłącznie publiczne napiętnowanie sprawców nie przynosi widocznych rezultatów. Ataki stają się coraz częstsze i bardziej powszechne. Pomimo tego, że prawo międzynarodowe aplikuje się do działań prowadzonych w cyberprzestrzeni, a wiele podmiotów dąży do wypracowania dodatkowych norm odpowiedzialnego zachowania w cyberprzestrzeni, sytuacja staje się coraz bardziej poważna, a agresorzy nie mają zahamowań. Przykładem są choćby masowe ataki na instytucje z sektora zdrowia w czasach pandemii COVID-19. Zastosowanie konkretnych i efektywnych działań jest także kluczowe z punktu widzenia wiarygodności. Nałożenie sankcji jest ważnym krokiem, pokazującym, że UE poza wymiarem deklaratywnym i normatywnym proponuje skuteczne działania, które mogą przyczynić się do kształtowania areny międzynarodowej, także jeśli chodzi o środowisko cyberprzestrzeni.

POTENCJAŁ GRACZY I MOŻLIWOŚCI OD STRASZANIA

Problem atrybucji oraz dotychczasowego braku reakcji przynosi trudność w efektywnym zastosowaniu klasycznych koncepcji i teorii z obszaru bezpieczeństwa międzynarodowego, takich jak na przykład koncepcji odstraszania. Odstraszanie uważa się za jedną z funkcji systemu obronnego państwa, której istota polega na zniechęcaniu strony przeciwnej do podejmowania działań, które byłyby niekorzystne z punktu widzenia danego podmiotu[7]. Jedną z form zniechęcania jest groźba odwetu, świadomość agresora o możliwości poniesienia wysokich kosztów za podejmowane działania[8]. Inną metodą jest zaburzanie „kalkulacji zysków" agresora albo poprzez zwiększenie kosztów ataku (np. przez zastosowanie skutecznych zabezpieczeń), albo przez zniwelowanie skutków ataku (budowanie wysokiego stopnia odporności na ataki)[f]. Skuteczny odwet uzależniony jest zarówno od właściwej atrybucji, jak i posiadania narzędzi, którymi można ukarać sprawcę. Paleta narzędzi w zależności od podmiotów może być różna: od wspomnianego wcześniej publicznego napiętnowania agresora (jak pokazuje historia, działanie niekoniecznie skuteczne), przez sankcje, aż po zastosowanie działań ofensywnych, zarówno kinetycznych, jak i cyfrowych. Te ostatnie są głównym przedmiotem tego tekstu i dlatego poniżej przedstawiony zostanie przegląd krajobrazu podejścia do budowy ofensywnych środków cyfrowych i trudności związanych z tym obszarem.

f Więcej o koncepcjach odstraszania w cyberprzestrzeni: Nye J. S., *Deterrence and Dissuasion in Cyberspace*, International Security, 43:3 (Winter, 2016/2017), s. 44-71.

NATO, potwierdzając w 2014 roku na Szczycie w Walii, że atak cyfrowy może przynieść aktywację art. 5 Traktatu Waszyngtońskiego, uznało, że cyberobrona jest integralnym elementem obrony kolektywnej. Potencjalni rywale otrzymali zatem wyraźny sygnał – bierzcie pod uwagę potencjalne konsekwencje. Przez długi czas w arsenale ofensywnych odpowiedzi na atak brakowało środków cyfrowych. NATO skupiało się na ochronie własnych sieci i systemów teleinformatycznych, nie dopuszczając stosowania aktywnych środków ofensywnych. Potencjalną formą odpowiedzi były zatem kinetyczne środki odwetowe. Paradoksalnie brak mniej inwazyjnych mechanizmów (za takie uznać można działania w cyberprzestrzeni) osłabiały zdolność odstraszania. Agresorzy kalkulują i wiedzą, że użycie siły fizycznej wiązałoby się z brzemiennymi konsekwencjami, zatem umiejętne manewrowanie poniżej progu wojny może doprowadzić do praktycznego braku konsekwencji[9]. Z czasem podejście to zaczęło się zmieniać. I choć Sojusz nadal bardzo mocno podkreśla, że ofensywne operacje w cyberprzestrzeni nie będą prowadzone ani przez personel NATO, ani pod flagą NATO[10], dopuszcza się, dla zwiększenia bezpieczeństwa, możliwość skorzystania z indywidualnych zdolności, które znajdują się w arsenale poszczególnych państw członkowskich. Kraje takie jak Wielka Brytania, Stany Zjednoczone, Holandia, Estonia i Dania dobrowolnie zgłosiły swoją gotowość do wsparcia ofensywnych działań. Rolą Sojuszu byłaby głównie ich koordynacja[11]. Rozbudowa indywidualnych arsenałów ofensywnych działań w cyberprzestrzeni, a także zmiana na poziomie doktrynalnym jest obserwowana w wielu krajach. Wspomniane wcześniej Stany Zjednoczone są flagowym przykładem. Państwo to nie tylko wiele inwestuje w rozwijanie zdolności, ale także zmienia podejście, promując aktywne neutralizowanie działań adwersarzy już w ich własnych systemach, sieciach. Podejście to nosi nazwę *defending forward* i dobrze ilustruje zmianę myślenia o zapewnianiu bezpieczeństwa cyfrowego. Wedle nowego modelu skuteczna obrona silnie koreluje z możliwościami działań ofensywnych.

Uwolnienie cyfrowej opcji odwetowej z punktu widzenia budowania siły odstraszania NATO jest działaniem bardzo korzystnym. Po pierwsze cyfrowy atak prowadzony na systemy teleinformatyczne może być działaniem bardziej proporcjonalnym[12]. Z drugiej strony, jak zostało zasygnalizowane, poszerzony został wachlarz możliwych opcji do działania, co wpłynąć może na kalkulacje agresorów.

Kolejnym warunkiem realnej zmiany zachowania agresora jest jego przekonanie, że arsenał, jakim dysponuje rywal, jest poważny i będzie skuteczny. Jeśli podmiot uwierzy w to, że może ponieść realne straty, może stracić zapał do ataku. Komunikacja siły, ustalenie realnego potencjału jest zatem istotną funkcją odstraszania. To także ważna wiedza dla wyboru właściwej strategii obrony – im więcej wiemy o arsenale rywala, tym lepiej jesteśmy w stanie się przygotować. Natura cyberprzestrzeni i narzędzi cyfrowych utrudnia działania związane z oceną potencjału innych graczy. Ofensywnych narzędzi cyfrowych nie pokazuje się na paradach wojskowych, nie można ich policzyć, a państwa niechętnie chwalą się tym, czym dysponują[g]. Wiedze czerpie się z obserwacji albo z działań wywiadowczych, a czasem z przecieków. Wszystko to ma konsekwencje dla środowiska bezpieczeństwa. Niepewność, błędna kalkulacja może prowadzić do **niekontrolowanego wyścigu cyfrowych zbrojeń, nowej odsłony klasycznego dylematu bezpieczeństwa.**

Wszystko to przywiodło nas do wniosku, od którego rozpoczął się ten tekst – państwa masowo rozwijają swoje zdolności do działań w cyberprzestrzeni. Przytoczone wcześniej wspólne oświadczenie szefów agencji wywiadowczych USA przybliża ocenę cyfrowej siły wybranych aktorów, rywali USA, a tym samym NATO:

- Rosja jest podmiotem dysponującym pełnym zakresem możliwości działań w cyberprzestrzeni, stanowiącym główne zagrożenie dla bezpieczeństwa USA. Posiada bardzo zaawansowany ofensywny program oraz zaawansowane rozwiązania proceduralne. Taką ocenę potencjału potwierdzają przykłady wrogich kampanii z ostatnich lat.

- Chiny coraz mocniej zwiększają swoje możliwości do działań prowadzonych w cyberprzestrzeni, a co za tym idzie, coraz trudniej się przed nimi bronić. Ofensywne wysiłki Chin skoncentrowane są na pozyskiwanie informacji oraz na działania, które mają za zadanie zapewnić bezpieczeństwo trwania reżimu.

- Iran aktywnie wykorzystuje cyberprzestrzeń do szpiegostwa, działań propagandowych, a także ataków na konkretne systemy komputerowe. Działania są nakierowane zarówno na USA, jak i sojuszników USA w regionie Bliskiego Wschodu.

- Korea Północna dysponuje środkami pozwalającymi skutecznie zakłócać bezpieczeństwo rywali, a służy to głównie realizacji celów politycznych tego kraju. Jak pokazują wydarzenia z przeszłości, Korea ma przynajmniej zdolność do szeroko zakrojonych operacji szpiegowskich i naruszających integralność danych i systemów.

CYFROWE BEZPIECZEŃSTWO PAŃSTW NATO

Oczywiście potencjał do prowadzenia działań w cyberprzestrzeni rozwijają także kraje NATO. Na szczycie Sojuszu w Warszawie w 2016 ogłoszona została decyzja o uznaniu cyberprzestrzeni jako domeny działań wojennych, oraz przyjęte zostało wezwanie do wzmacniania potencjału państw członkowskich zawarte w tak zwanym Cyber Defence Pledge. Przyspieszyło to znacznie proces budowania militarnych zdolności państw członkowskich do działania w cyberprzestrzeni[h]. Polska jest jednym z krajów, która bardzo intensywnie przystąpiła do realizacji tego zadania. Rozpoczęto proces tworzenia Wojsk Obrony Cyberprzestrzeni, którego zakończenie przewiduje się na rok 2024[13]. Mają one działać w całym spektrum, a zatem działać zarówno ofensywnie, jak i defensywnie.

Nie tylko państwa członkowskie, ale samo NATO wzmacnia swoje cyberbezpieczeństwo. Wiąże się to ze zmianami instytucjonalnymi, organizacyjnymi, proceduralnymi, modyfikacjami w strukturze dowodzenia i kierowania. W ostatnim czasie przełomowymi działaniami było przyjęcie doktryny poświęconej prowadzeniu działań w cyberprzestrzeni (AJP 3.20 Cyberspace Operations) oraz utworzenie podmiotu kluczowego dla operacyjnych działań prowadzonych w cyberprzestrzeni: Cyberspace Operations Center[i]. NATO stara się nadążać za zmianami w środowisku cyfrowym także na poziomie koncepcyjnym. Niedawno pod auspicjami Sekretarza Generalnego NATO zainicjowany został proces refleksji nad przyszłością strategiczną Sojuszu. Proces ma zakończyć się w 2021 roku i spodziewać się można, że kwestie dotyczące cyberbezpieczeństwa oraz nowych technologii będą wysoko na agendzie. Dodatkowo do życia powołana została Grupa Doradcza ds. nowych technologii, która wesprze proces strategicznego planowania rozbudowy potencjału technologicznego Sojuszu. Warto zauważyć, że w obu grupach Polska ma swoją ekspercką reprezentację.

g Nie istnieje dużo publicznie dostępnych informacji o zastosowaniu środków ofensywnych w cyberprzestrzeni. Dodatkowo ich wartość, skuteczność zmienia się w czasie.

h Przede wszystkim w obszarze obrony, w niektórych przypadkach także możliwości ofensywnych.

i Jego główne zadania to: zapewnienie świadomości sytuacyjnej w cyberprzestrzeni, planowanie sojuszniczych operacji w cyberprzestrzeni, zarządzanie ich wykonywaniem. *NATO to integrate offensive cyber capabilities of individual members*, Fifth Domain, 28.05.2019, [online:] https://www.fifthdomain.com/international/2019/05/28/nato-to-integrate-offensive-cyber-capabilities-of-individual-members/.

Oczywiście NATO, pomimo dużego postępu w zakresie wzmacniania swoich cyfrowych możliwości, wciąż mierzy się z wieloma trudnościami. Poziom bezpieczeństwa i zdolności między poszczególnymi państwami członkowskimi wciąż jest nierówny (co osłabia całość systemu), konieczne jest usprawnianie mechanizmów zwiększających świadomość sytuacyjną, w tym rozbudowa tak zwanych „wskaźników i ostrzeżeń”[14], konieczna jest lepsza koordynacja i doprecyzowanie procedur związanych przede wszystkim z działaniami ofensywnymi[15]. Dodatkowo, jak wskazują Nicolas Mazzucchi i Alix Desforges, sojusznicy powinni opracować krajowe zasady zaangażowania zgodne z zasadami prawa międzynarodowego oraz wszyscy sojusznicy NATO muszą zapewnić, że będą one zgodne z uzgodnionym podejściem sojuszu do cyberobrony. Obecnie różne kraje mają różne poglądy szczególnie na ofensywne działania[16].

CYFROWY GAME CHANGER

Cyberatak na systemy NATO lub jego państw członkowskich może przynieść poważne zagrożenie dla ich bezpieczeństwa, powodzenia prowadzonych działań i misji. Silne ucyfrowienie i zaawansowany rozwój technologiczny, uznawane za przewagę, paradoksalnie mogą zostać wykorzystane przez teoretycznie słabszych rywali. Zastosowana może zostać asymetryczna metoda uderzenia w wrażliwe punkty, które mogą mieć wpływ na przebieg konfliktu. Rozwiązania cyfrowe, które nie sposób w pełni zabezpieczyć, mogą stanowić piętę achillesową. Jak wskazują eksperci, strategia ta rozpatrywana jest choćby przez Chiny. W przypadku starcia z wojskami USA, Chiny planują użyć środków cyfrowych do ataku na strategiczne cele po to, aby osłabić przeciwnika i zmniejszyć przewagę USA[17].

Na tym etapie operacje ofensywne zapewne nie przesądzą o wyniku całego potencjalnego konfliktu militarnego[j], ale mogą znacznie wpłynąć na jego przebieg. Zneutralizowanie działania systemu obrony przeciwlotniczej (szczególnie w pierwszej fazie konfliktu), sparaliżowanie logistyki, zakłócenie działania coraz silniej zinformatyzowanych systemów uzbrojenia czy też naruszenie funkcjonowania systemu kontroli i dowodzenia mogą mieć poważne konsekwencje. Nie można także pominąć wpływu potencjalnych kampanii psychologicznych wykorzystujących cyberprzestrzeń do działań propagandowych, dezinformacyjnych czy manipulacyjnych. Mogą one oddziaływać na morale walczących, kształtować opinię publiczną, która przecież determinuje mocno wybory polityczne decydentów[18].

Myśląc o obronie i zagrożeniach, nie należy przeoczyć potencjalnych korzyści wynikających z możliwości, jakie dają ofensywne środki cyfrowe. Z punktu widzenia państw NATO skuteczne kampanie ofensywne nakierowane na systemy i sieci teleinformatyczne wykorzystywane przez rywala mogą zniwelować jego atuty w postaci na przykład środków izolowania pola walki (A2AD)[k]. Rosyjskie rozwiązania A2AD stosowane w rejonie Kaliningradu, ale i na Krymie, Arktyce, w Syrii, stanowią poważne wyzwanie dla NATO[19]. Możliwość ich neutralizacji mogłaby mieć niebagatelne znaczenie dla przebiegu potencjalnego konfliktu. Także strategiczne informacje zdobywane za pomocą cyberszpiegostwa mogą zmieniać świadomość sytuacyjną i podejmować strategicznie ważne decyzje.

Wszystko to pokazuje, jak **wielką wagę ma budowanie pozycji w cyberprzestrzeni. Jej siła polega na tym, że stanowiąc odrębną domenę, jest ona jednocześnie środowiskiem warunkującym funkcjonowanie wszystkich pozostałych: działań na lądzie, w wodzie, powietrzu czy kosmosie.** Zatem jest w żywotnym interesie państw, aby nie tylko zadbać o jej bezpieczeństwo, ale skutecznie i mądrze wykorzystywać siłę potencjału ofensywnego. Jednocześnie należy pamiętać rozbudowa potencjału ofensywnego musi być postrzegana przez pryzmat całego środowiska bezpieczeństwa i musi być prowadzona odpowiedzialnie. Atak „WannaCry” pokazał, że narzędzia cyfrowe, które gromadzą państwa, oraz wiedza o podatnościach mogą wpaść w ręce tych, którzy wykorzystają je do niszczycielskich działań. Jest to problem, który musi stać się przedmiotem powszechnej debaty. Cyberbezpieczeństwo jest kluczowym warunkiem niezakłóconego funkcjonowania i rozwoju wszystkich państw i społeczeństw. Należy zatem wspólnie zadbać o stabilność i bezpieczeństwo funkcjonowania cyberprzestrzeni.

Przedstawione wnioski dotyczące roli ofensywnych działań prowadzonych w cyberprzestrzeni są istotne także dla krajów regionu Trójmorza. Wspomniane wcześniej (oraz w rozdziale jedenastym) możliwości cyfrowego oddziaływania na zdolności A2AD jasno pokazują, jak istotne znaczenie ma cyberbezpieczeństwo dla stabilności wschodniej flanki NATO. To zaledwie przykład tego, jak cyberataki mogą oddziaływać na stabilność regionu. Dezinformacja, szpiegostwo, zakłócanie funkcjonowania infrastruktury krytycznej – wszystkie te wrogie działania zyskują nowe znaczenie, gdy są prowadzone w środowisku cyfrowym. Z punktu widzenia przeciwdziałania wyzwaniu konieczne jest inwestowanie w budowę zdolności cyfrowych. zarówno w wymiarze defensywnym, jak i ofensywnym, na poziomie poszczególnych państw. Dodatkowo kluczowe jest jeszcze silniejsze wzmacnianie potencjału NATO w obszarze cyfrowym. Większa spójność w rozpoznawaniu zagrożeń, budowaniu świadomości sytuacyjnej, jeszcze skuteczniejsza koordynacja działań i zdecydowana odpowiedź na wrogie działania w cyberprzestrzeni (szczególnie na poziomie politycznym) to kierunek, który powinny wspierać wszystkie państwa regionu. Szczególnie, że to właśnie one znajdują się w krytycznym obszarze geopolitycznego teatru działań.

j Choć, jak pokazuje rozdział jedenasty, w przyszłości ocena ta może ulec zmianie.

k Ang. Anti-access Area Denial. Wątek ten poruszony także zostanie w rozdziale jedenastym.

PRZYPISY

1 Por. Uren T., Hogeveen B., Hanson F., *Defining offensive cyber capabilities*, [online:] https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

2 Smeets M., Lin H. S., *Offensive Cyber Capabilities: To What Ends?*, NATO CCD COE Publications, 2018.

3 *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, University of Washington, 11.10.2017, [online:] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

4 *UK and allies reveal global scale of Chinese cyber campaign*, GOV.UK, [online:] https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign.

5 *China Knows All About the F-35 and F-22 (Thanks to the Data It Stole)*, The National Interest, [online:] *https://nationalinterest.org/blog/buzz/china-knows-all-about-f-35-and-f-22-thanks-data-it-stole-61912*.

6 Moret E., Pawlak P., *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?*, European Union Institute for Security Studies (EUISS), s. 2.

7 *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, 2009.

8 Lewis J. A., *Cross-Domain Deterrence and Credible Threats*, CSIS, 07.2010, [online:] https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100701_Cross_Domain_Deterrence.pdf.

9 Uren T., Hogeveen B., Hanson F., *Defining offensive cyber capabilities*, ASPI, 04.07.2018, [online:] https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

10 Lewis D., *What is NATO really doing in cyberspace?*, War on the Rocks, 04.02.2019, [online:] https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/.

11 Tamże.

12 Por. Schmitt M., *The Law of Cyber Targeting*, Tallinn Paper No.7, 2015, s. 18.

13 *Zdzikot: Wojska Obrony Cyberprzestrzeni osiągną gotowość w 2024 r.*, Defence 24, 04.10.2019, [online:] https://www.defence24.pl/zdzikot-wojska-obrony-cyberprzestrzeni-osiagna-gotowosc-w-2024-r.

14 *Operationalizing Cyberspace as a Military Domain*, RAND, 06.2012.

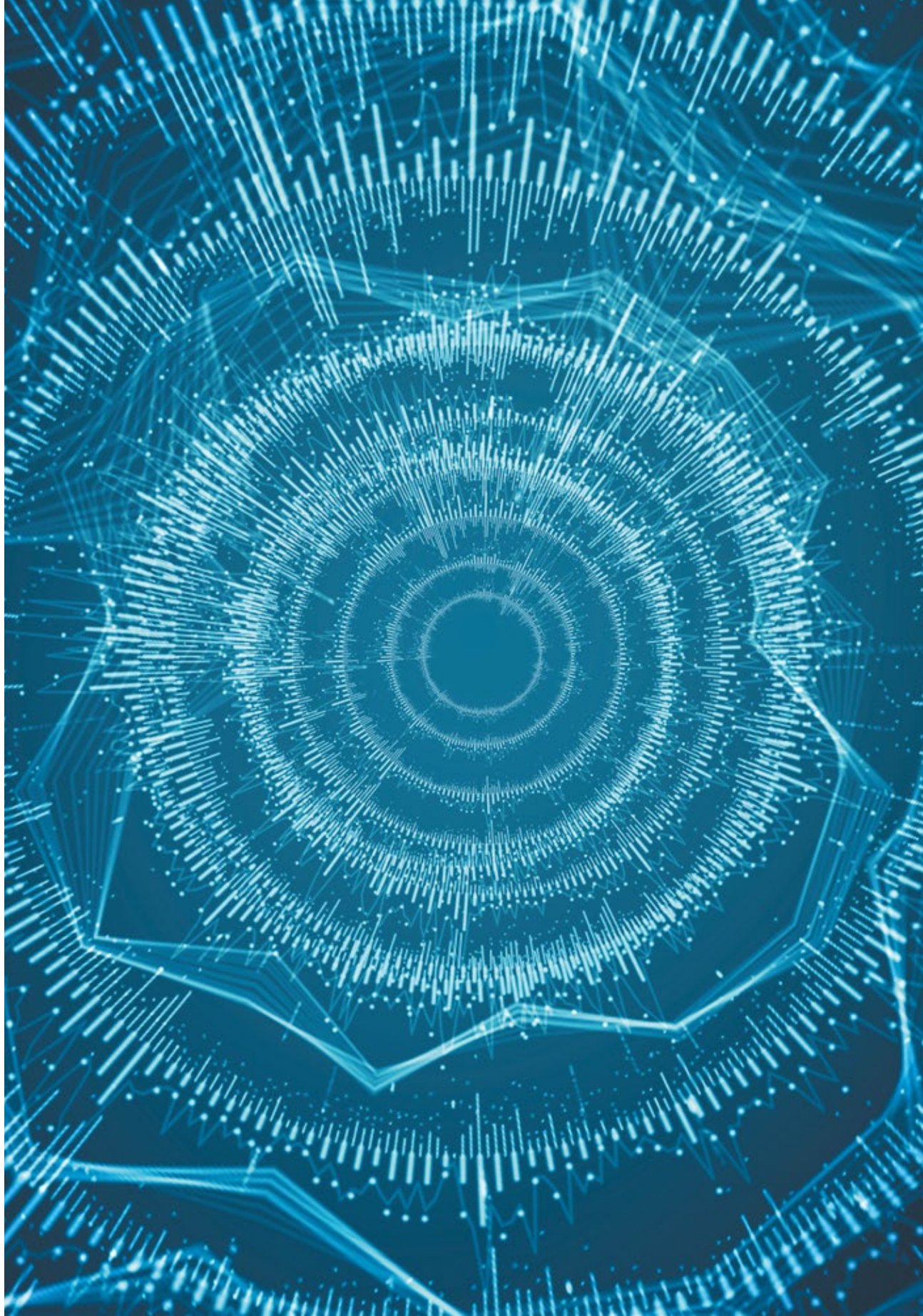
15 Smeets M., *NATO Allies Need to Come to Terms With Offensive Cyber Operations*, Lawfare, 14.10.2019 [online:] https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations; *Here are the problems offensive cyber poses for NATO*, Fifth Domain, 20.11.2019 [online:] https://www.fifthdomain.com/international/2019/11/20/here-are-the-problems-offensive-cyber-poses-for-nato/.

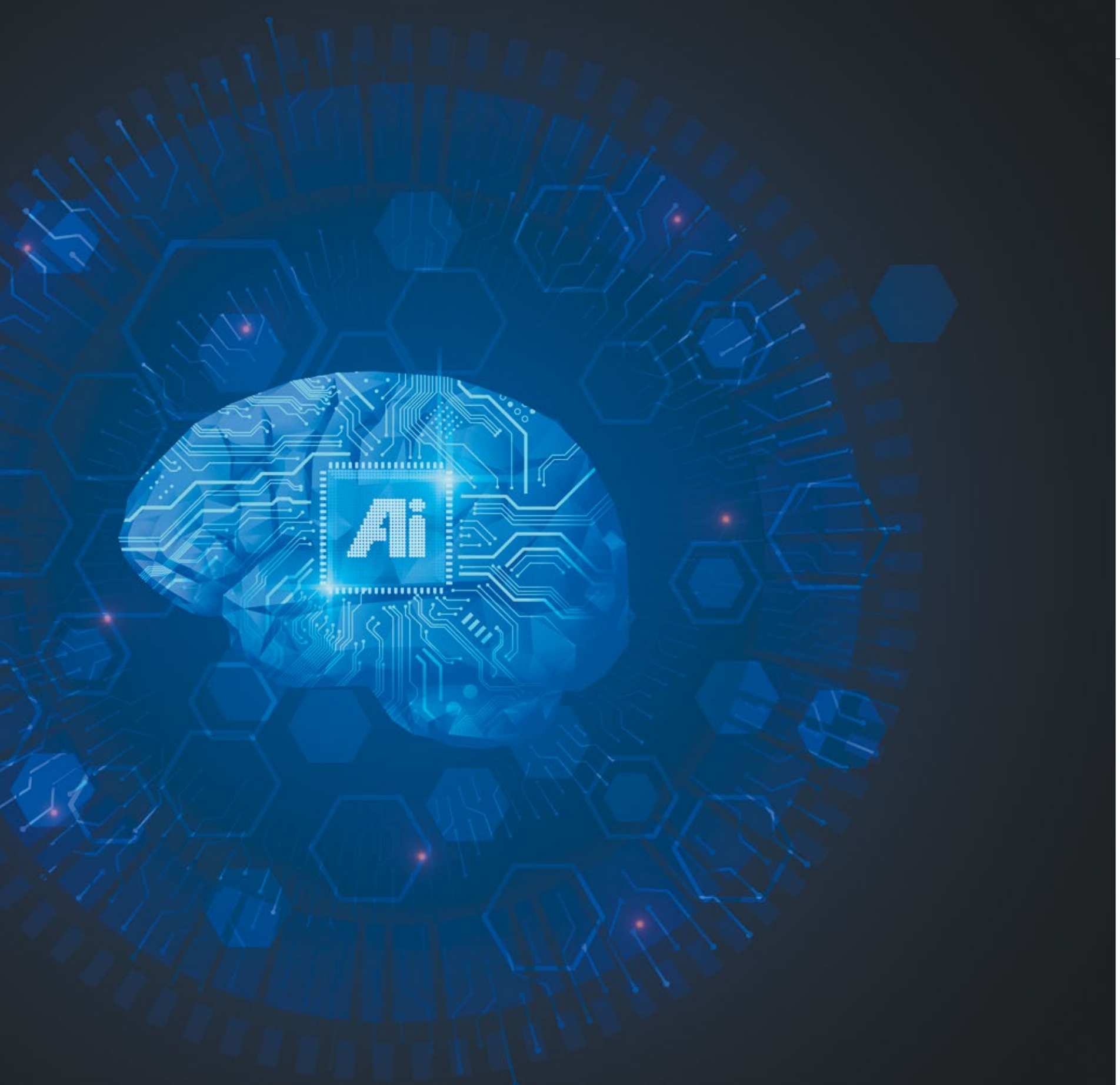
16 Mazzucchi N., Desforges A., *Web Wars: Preparing for the Next Cyber Crisis*, Carnegie Europe, 28.11.2019, [online:] https://carnegieeurope.eu/2019/11/28/web-wars-preparing-for-next-cyber-crisis-pub-80420.

17 Austin G., Gady F., *Cyber Détente between the United States and China: Shaping the Agenda*, East West Institite, 2012, s. 15.

18 Lewis J. A., T*he Role of Offensive Cyber Operations in NATO's Collective Defence*, Tallinn Paper No. 8, 2015, s. 4-5.

19 *Rosyjskie zdolności w zakresie środków izolowania pola walki (A2AD) – wnioski dla NATO*, Defence 24, [online:] https://www.defence24.pl/rosyjskie-zdolnosci-w-zakresie-srodkow-izolowania-pola-walki-a2ad-wnioski-dla-nato.





Dr Joanna Świątkowska

SZTUCZNA INTELIGENCJA – PALIWO GEOPOLITYCZNYCH ZMIAN

Sztuczna inteligencja (SI, od ang. *artificial intelligence*)[a] jest technologią ogólnego zastosowania, czyli taką, która fundamentalnie zmienia sposób funkcjonowania całych sektorów. W konsekwencji będzie ona warunkować stan globalnej gospodarki, rozwój dalszych przełomowych technologii i modeli biznesowych, jak również wpłynie na obszar bezpieczeństwa międzynarodowego. Choć na tym etapie nie sposób przewidzieć w pełni konsekwencji rozwoju SI, już teraz można stwierdzić, że będzie miała ona strategiczne znacznie, wpływając na balans sił i rywalizację między kluczowymi graczami globalnej areny.

1. DLACZEGO SI WPŁYNIE NA GEOPOLITYCZNY PORZĄDEK

W ostatnich latach, głównie dzięki postępom w dziedzinie uczenia maszynowego związanym z wykorzystywaniem sieci neuronowych, bardzo silnie rozwinęły się możliwości i potencjał SI. Niektórzy nawet twierdzą, że jest to najważniejsza technologia, jaka kiedykolwiek została wynaleziona[1]. Nie uszło to uwadze kluczowych graczy takich jak UE, Chiny, USA, Rosja. Podmioty te uczyniły rozwój zdolności w tym obszarze strategicznym priorytetem. Dziś już wiadomo, że SI będzie coraz silniej wpływać na rywalizację mocarstw, będzie

a Nie istnieje jedna ogólnie przyjęta definicja tego, czym jest sztuczna inteligencja. Często spotykanym podejściem jest rozumienie AI jako zdolności maszyn do realizowania działań przypisywanych ludzkiej inteligencji. W niniejszym artykule AI będzie używane jako nazwa zbiorcza dla wielu technologii i podejść pozwalających rozwiązać wybrane problemy, rozwiązać określone zadania. Jednym z tych podejść, do którego najczęściej referować będzie tekst, jest uczenie maszynowe oparte na sieciach neuronowych.

determinować pozycję poszczególnych graczy i tym samym kształtować sytuację geopolityczną.

Co ciekawe, jednym z przełomowych momentów, które silnie przyśpieszyły światowy wyścig w ramach rozwoju SI, był rok 2017, kiedy to maszyna AlphaGo odniosła zwycięstwo nad jednym z najlepszych w historii graczy w go. Zwycięstwo to było symboliczne, bowiem go to chińska, uznawana za najstarszą na świecie strategiczna gra planszowa, która charakteryzuje się koniecznością bardzo logicznego, wielowymiarowego myślenia. Triumf komputera nad człowiekiem był momentem wstrząsu, który uruchomił lawinę wysiłków Chin do działania w obszarze sztucznej inteligencji, co w konsekwencji przyśpieszyło globalną rywalizację[2]. Sławna stała się także wypowiedź prezydenta Rosji Władimira Putina z tamtego okresu, który powiedział, że ten, kto będzie rządził sztuczną inteligencją, będzie rządził światem[3].

Siła SI wynika przede wszystkim z tego, że w nadchodzących latach będzie ona silnikiem napędowym ekonomii, innowacji, kolejnych faz rozwoju technologicznego. Dodatkowo zdeterminuje silnie środowisko bezpieczeństwa.

SI jako fundament nowoczesnych cyfrowych gospodarek zwiększy efektywność procesów produkcyjnych i usług, produktywność, innowacyjność, powstawanie nowych rozwiązań technologicznych i modeli biznesowych. Szacuje się, że do 2030 r. wkład SI w globalną gospodarkę wyniesie 15,7 bln USD[4]. Zrewolucjonizowane zostaną wszystkie sektory: transport przyszłości oparty na pojazdach autonomicznych, zaawansowane analizy rynków finansowych, wydajniejsze rolnictwo, bardziej efektywna i zwinna produkcja, transformacja ekologiczna – to wyłącznie przykłady wpływu SI. Epidemia COVID-19 wyraźnie pokazała potencjał SI we wspieraniu sektora zdrowia: diagnozowaniu chorób, ich rozprzestrzenianiu się, przewidywaniu rozwoju.

W wyścigu związanym z rozwojem i implementacją SI gracze, którzy będą spóźnieni, zaryzykują utratę pozycji w globalnej gospodarce, w światowym łańcuchu wartości. Większość zatem stara się nie wypaść z gry i coraz więcej inwestować w rozwój swego potencjału. Co więcej trwa rywalizacja o to, kto będzie pierwszy, kto zainicjuje procesy, standardy i rozwiązania, które ukształtują ekosystem. To pozwoli czerpać korzyści wynikające z ustanowienia „reguł gry".

Obok gospodarki drugim obszarem, gdzie SI będzie wpływało na kształt geopolityki, jest bezpieczeństwo. SI będzie silnie determinowało bezpieczeństwo narodowe poszczególnych podmiotów. Zarówno w wymiarze wewnętrznym, jak i przede wszystkim zewnętrznym. Pomimo początkowej fazy rozwoju SI już teraz w obszarze militarnym wdraża się wiele rozwiązań na niej opartych. Eksperci wskazują, że wraz z dalszym jej rozwojem będziemy świadkami całkowitej zmiany myślenia w sposobie prowadzenia konfliktów, w transformacji pola walk – zarówno na poziomie taktycznym, operacyjnym, jak i strategicznym.

Zastosowanie SI w wymiarze militarnym jest bardzo rozległe. SI może między innymi wspierać działania związane z wywiadem i rozpoznaniem (m.in. gromadzenie olbrzymich mas danych i ich zaawansowana analiza), znacznie podnosząc wielodomenową świadomość sytuacyjną. Jest to kluczowa technologia dla szeroko rozumianego rozwoju i koordynacji pracy systemów bezzałogowych (m.in. swarming). Odegra bardzo istotną rolę w modelowaniu i symulowaniu pola walki, a także prowadzeniu zaawansowanych gier wojennych.

SI już teraz pozwala precyzyjnie rozpoznawać i namierzać cele. Przekłada się to na to, że wpływa na zwiększenie możliwość skutecznego uderzenia w aktywa strategiczne, takie jak lotniskowce, pociski mobilne lub nawet broń nuklearną[5]. Jak wskazuje Zachary S. Davis, rewolucjonizując funkcjonowanie BMC3I[b], SI może przynieść zmiany na

b Zarządzanie walką/dowodzenie, kontrola, łączność i rozpoznanie. (ang. Battle Management, Command, Control, Communications and Intelligence).

poziomie strategicznym. Koordynując i wspierając działania wielu platform, może np. pomóc rozpoznawać, identyfikować i namierzać rozmieszczone systemy rakietowe. Ma zatem potencjał stać się istotnym elementem wykorzystywanym w przeciwdziałaniu strategii izolacji pola walki (A2AD) stosowanej przez Rosję i Chiny w Europie i Azji[6].

Biorąc powyższe pod uwagę, można zaryzykować śmiałe stwierdzenie, że rozwój i zastosowanie SI może doprowadzić nawet do naruszenia równowagi strategicznej[c], prowadzić do eskalacji konfliktów, a tym samym zwiększyć ryzyko wojny.

SI ma zastosowanie nie tylko w walce konwencjonalnej. W przyszłości (do pewnego stopnia procesy te obserwowane są także teraz) przyczyni się do zmiany oblicza walki informacyjnej, wprowadzając działania dezinformacyjne i manipulacyjne na zupełnie inny, wyższy poziom zaawansowania. Rozwój i coraz częstsze zastosowanie choćby technologii *deepfake* jest dobrą egzemplifikacją problemu. Oddziaływanie psychologiczne także będzie miało istotny wpływ na przebieg konfliktów militarnych[d].

Wykorzystanie SI do przeprowadzania zaawansowanych cyberataków spotęguje już poważne problemy związane z zapewnianiem cyberbezpieczeństwa. Dzisiejsze trudności związane z ochroną systemów i sieci teleinformatycznych w erze SI będą mierzyły się z jeszcze trudniejszymi wyzwaniami. Infrastruktura krytyczna, kluczowe systemy będą jeszcze mocniej zagrożone.

Wszechstronne zastosowanie SI budzi wiele obaw natury etycznej. Niezamierzone wady i błędy technologii prowadzące m.in. do dyskryminacji, uprzedzeń, niesprawiedliwych i błędnych decyzji, ale także intencjonalne nadużycia, np. w formie inwigilacji lub zaawansowanych kampanii dezinformacyjnych prowadzonych przez reżimy autorytarne, wywołują reakcje w postaci coraz większej ilości inicjatyw mających na celu wypracować standardy i rekomendacje etyczne dla rozwoju i wykorzystania SI[e].

2. UKŁAD SIŁ

2.1. Chiny

O ile zwycięstwo programu komputerowego nad człowiekiem było momentem przebudzenia Chin i doprowadziło do ofensywy w rozwoju SI, tak z kolei rozpędzone chińskie działania w połączeniu z rozbudzonymi apetytami Rosji wzbudziły niepokój świata, przede wszystkim USA. Uśpieni swymi osiągnięciami i dominacja technologiczną Amerykanie na początku nie doceniali konkurencji. Tymczasem Chiny inwestowały coraz więcej, pozyskiwały specjalistów, zgłaszały coraz więcej patentów, intensyfikowały badania naukowe[f]. Rok 2030 został wskazany jako moment, gdy Chiny mają stać się najważniejszym centrum innowacyjności w zakresie SI[7]. Wola polityczna i strategiczne, holistyczne podejście zaczęło przynosić efekty. Na wyobraźnię musi podziałać fakt, że Chiny zanotowały „30-krotny wzrost całkowitego finansowania B+R w latach 1991–2015 i przewiduje się, że w ciągu 10 lat przeskoczą USA w zakresie absolutnych wydatków w tym obszarze"[8].

c Istnienie wspólnych podatności oraz zagwarantowanego odwetu jest podstawą wywodzącej się z teorii odstraszania doktryny wzajemnie zagwarantowanego zniszczenia. W momencie, gdy możliwe jest dokonanie ataku na cele strategiczne (np. na NC3) oraz zneutralizowanie działań odwetowych – zmienia to percepcję i myślenie o równowadze strategicznej. Więcej Davis Z. S., *Artificial Intelligence on the Battlefield. An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise*, LLNL, 03.2019.

d Więcej o tym w rozdziale dziesiątym poświęconym ofensywnym zdolnościom.

e Wyłącznie kilka przykładów to: The Ethics Guidelines for Trustworthy Artificial Intelligence przygotowany przez High-Level Expert Group on Artificial Intelligence; Toward a Draft Text of a Recommendation on the Ethics of Artificial Intelligence przygotowany przez Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence.

f Przewiduje się, że już w 2025 Chiny mogą przegonić USA w zakresie ilości najczęściej cytowanych prac naukowych poświęconych AI. *Interim Report*, National Security Commission on Artificial Intelligence, 2019, s. 17.

Chiny przez wiele lat postrzegane jako mało innowacyjny kraj, „podwykonawca" świata. Chińscy decydenci bardzo świadomie zdecydowali się to zmienić i rozpoczęli konsekwentne realizowane kolejnych etapów modernizacji technologicznej. Wyżej wymienione działania i inwestycje mają szansę przynieść założony efekt szczególnie w połączeniu z naturalnymi przewagami, które charakteryzują Chiny. Efekt skali czy dostęp do olbrzymich ilości danych (paliwa SI) sprawia, że chińskie podmioty mają bardzo dogodną pozycję do rozwijania technologii i masowych wdrożeń SI[9]. Plany Pekinu wykraczają jednak poza wzmacnianie potencjału gospodarczego dzięki sztucznej inteligencji. W swym podejściu stawiają bardzo silnie na rozwój militarnego wykorzystania SI[g]. Służą temu różne działania, między innymi zacieśnianie współpracy wojska z cywilami (tak zwane *Military-Civil Fusion*)[10]. W materiałach opisujących wizję Chin eksperci podkreślają, że rysuje się propozycja nowego modelu modernizacji militarnej opartej na osiągnięciu „inteligencji na polu walki" (oryginalnie koncepcje na angielski tłumaczy się jako *intelligentization*)[11]. Dzięki przejściu technologicznej rewolucji Chiny mogą znacznie rozbudować swój potencjał wojskowy, co może mieć globalne konsekwencje.

2.2. Rosja

Rosja, podobnie do Chin, prezentuje bardzo ambitne podejście do rozwoju SI, ze szczególnym uwzględnieniem jej wykorzystania w wymiarze militarnym. W październiku 2019 roku ogłoszona została Strategia SI, która ma stanowić drogowskaz pozwalający osiągnąć strategiczne cele[12]. Panuje wiele różnych opinii na temat realnego potencjału Rosji w obszarze SI. Z jednej strony widać bardzo wyraźnie determinację w dążeniu do jej rozwoju. Prezydent Putin postawił konkretne oczekiwania: Rosja ma być liderem w obszarze SI w 2025 roku[13].

Uruchomiło to wiele inicjatyw, m.in. powstają nowe rozwiązania instytucjonalne i organizacyjne (np. powołanie do życia the Elite Russian Army Academy[14] – elitarnej jednostki mającej być motorem napędowym innowacji w rosyjskiej armii), zintensyfikowane zostały działania w obszarze B+R, edukacji, a także zdynamizowania sektora prywatnego (np. program Go Russia!)[15]. Z drugiej jednak strony wysiłki te spotykają olbrzymie trudności, stawiające wiele znaków zapytania co do osiągnięcia ostatecznego sukcesu. Systemowe problemy takie jak trudności ekonomiczne, utrata ekspertów i talentów na rzecz zagranicznych przedsiębiorstw, korupcja, słabnący sektor nowych technologii stanowią duże wyzwanie[16].

O ile więc Rosji samodzielnie trudno będzie pokonać przeszkody, pojawiają się dodatkowe okoliczności, które sprawiają, że działania Moskwy trzeba brać bardzo poważnie. Potencjał Rosji może zostać znacząco wzmocniony zasobami partnerów, przede wszystkim Chin, z którymi Moskwa w ostatnim czasie bardzo silnie zacieśnia tak zwane „partnerstwo technologiczne", przede wszystkim w takich obszarach jak 5G czy też właśnie SI.

Współpraca nie ogranicza się do pobudzania innowacyjności (np. poprzez rozwój chińsko-rosyjskich parków naukowo-technicznych takich jak: Changchun Sino-Russian Science and Technology Park, centrum innowacji Skołkowo), wzajemnego wsparcia *stricte* technologicznego (np. przez dostarczanie pewnych technologii, specjalistów)[17], dzielenia się danymi, tworzeniem wspólnych funduszy na B+R. Ma ona także wymiar strategiczny. Dla obu państw równie istotne jest koordynowanie działań nakierowanych na kształtowanie standardów, decyzji międzynarodowych organizacji w obszarze nowych technologii. W kontekście współpracy warto wspomnieć, że Chiny i Rosje łączy jeszcze jeden ważny wątek związany z SI – oba kraje uznają go za ważne narzędzie służące kontroli obywateli, narzędzie, które ma pomóc władzy trwać niezakłócenie. Wspólne interesy i podejście zawsze cementują przymierza.

g Co charakteryzować będzie także opisane poniżej podejście rosyjskie.

Niezależnie od oceny realnego potencjału Rosji w rozwoju SI, już teraz jej dokonania w priorytetowym dla niej strategicznym obszarze obronności muszą budzić czujność. Istnieje wiele materiałów świadczących o intensywnym i wielowymiarowym stosowaniu SI w rosyjskim obszarze militarnym. SI znajduje zastosowanie między innymi w kontrolowaniu elementów zintegrowanego systemu obrony przeciwlotniczej (m.in. S-300, S-400); wspieraniu wielu funkcji związanych z uzbrojeniem i sprzętem bojowym (m.in. Su-35, helikoptery Mi-28N, czołgi T-14 Armata); SI odgrywa kluczową rolę w funkcjonowaniu pojazdów bezzałogowych, m.in. odpowiadając za ich nawigację, koordynację „działań w roju", prowadzenie wywiadu i rozpoznania, namierzanie celów[18]. SI jest także coraz mocniej wykorzystywana do planowania działań, przeprowadzania bardzo zaawansowanych gier wojennych. Wojsko rosyjskie wiele systemów wspieranych przez SI stosuje w Syrii, zbierając cenne lekcje i doświadczenia[19]. Wdrażanie rozwiązań SI do działań bojowych musi być silnie obserwowane przez NATO, a także szczególnie przez kraje Europy Środkowo-Wschodniej stanowiące wschodnią granicę Sojuszu.

2.3. USA

W najnowszym raporcie oceniającym amerykański potencjał w obszarze SI[20] przygotowanym przez specjalnie powołaną Komisję na zlecenie Kongresu zostało jasno wskazane, że rola USA jako globalnego lidera innowacji jest zagrożona[21]. W kontekście zastosowania SI w obszarze obronności ocena raportu jest jeszcze surowsza – mówi się bowiem, że przy braku działań, bądź też przy działaniach niewystarczających, może dojść do erozji przewagi militarnej USA nad rywalami[22]. Jak zostało powiedziane wcześniej, rozpędzone działania Chin w obszarze SI, w połączeniu z ich rozwojem innych krytycznych obszarów jak 5G, pchnęło USA do działania.

Pomimo alarmujących wniosków płynących z wyżej wymienionego raportu należy pamiętać, że USA jest ojczyzną topowych uniwersytetów, ośrodków badań nad sztuczną inteligencją, gigantów technologicznych, krajem przyciągających najlepsze talenty oraz innowatorów[23]. Potencjał jest ogromny. W dodatku rywalizacja międzynarodowa zmobilizowała działania na poziomie strategicznym, m.in. w 2019 Biały Dom wydał Rozporządzenie Wykonawcze dotyczące utrzymania amerykańskiej dominacji w obszarze SI[24], a w ciągu ostatnich 5 lat członkowie Kongresu przygotowali około 30 ustaw dotykających kwestii rozwoju SI. Również Departament Obrony Narodowej przyspiesza działania: powołano do życia Joint Artificial Intelligence Center (JAIC)[25] i rozpoczęto opracowywanie tak zwanej „strategii trzeciego offsetu", która ma pomóc dokonać kolejnego skoku modernizacyjnego amerykańskiej armii[26]. SI stało się kluczowym obszarem inwestycji Departamentu Obrony z prawie bilionem dolarów alokowanym w budżecie na 2020. Dodatkowo zaplanowano podwojenie budżetu JAIC do około 208 milionów dolarów z dużymi wzrostami już w 2021 roku[27]. Wiele projektów opartych na SI, takich jak projekt Maven, już jest realizowanych w ramach programów militarnych.

Prócz rozbudowy własnego potencjału, USA w ostatnich miesiącach bardzo silnie zaczęło orientować działania na rzecz osłabiania rywali, przede wszystkich Chin. Technologiczna wojna najbardziej widoczna jest w obszarze 5G, gdzie USA podejmuje wiele ostrych działań. Między innymi ograniczona została współpraca amerykańskich firm z Chinami po to, aby uniemożliwić transfer technologii[28]. Prawdziwym ciosem okazała się decyzja o odcięciu Chin od dostaw amerykańskich chipów[h]. Ten konkretny ruch może mieć bardzo poważne konsekwencje także dla rozwoju SI. Ofensywa amerykańska koncentruje się także na ograniczeniu dostępu do amerykańskich badań i wiedzy[29].

h Lub budowanych na bazie amerykańskich rozwiązań. Więcej: Świątkowska J., *The new U.S. chip rules – a game-changer in the 5G landscape?*, [online:] https://joannaswiatkowska.wordpress.com/2020/05/19/the-new-u-s-chip-rules-a-game-changer-in-the-5g-landscape/.

2.4. Unia Europejska

Unia Europejska (UE) rozumie strategiczny wymiar SI i podejmuje coraz więcej działań, aby być ważnym podmiotem w technologicznej grze[30]. Niemniej jednak stoi przed nią wiele bardzo poważnych wyzwań i ograniczeń, które sprawią, że droga ta nie będzie łatwa.

Naturalnie, z punktu widzenia UE, SI jest czynnikiem, który będzie kluczowy dla rozwoju jednolitego rynku cyfrowego – fundamentu całego rozwoju gospodarczego Unii. Dlatego też priorytetowe działania opisane niżej nakierowane są właśnie na pobudzenie potencjału rozwoju i wykorzystania SI. Jednak UE, mając bardzo silną pozycję regulacyjną i normatywną, koncentruje się także na kształtowaniu systemu związanego z SI – tworzeniu wytycznych i rekomendacji dotyczących przede wszystkim etycznego wymiaru SI[31]. Co ważne, ten drugi filar z punktu widzenia globalnego wpływu ma nie mniejsze znaczenie niż budowa potencjału technologicznego. Powinien być zatem dobrze wykorzystany[32].

Jak zostało wspomniane, w ramach rozwoju SI UE prowadzi szereg wielowymiarowych działań dążących do zwiększenia potencjału technologicznego i przemysłowego oraz wdrożenia SI w całej gospodarce. Aby to osiągnąć, przewidywane są między innymi znaczące inwestycje. W latach 2018–2020 Komisja zamierza zainwestować około 1,5 mld EUR m.in. w badania (w tym podstawowe i przemysłowe) i innowacje[33]. Planuje także pobudzać większe zaangażowanie prywatnych inwestycji w SI w ramach Europejskiego Funduszu Inwestycji Strategicznych (co najmniej 500 mln EUR w latach 2018–2020)[34]. Zwiększenie wydatków jest istotne, szczególnie, że – jak wskazuje unijna strategia SI – „Europa pozostaje w tyle w zakresie prywatnych inwestycji w SI, których wartość w 2016 r. wyniosła ok. 2,4–3,2 mld EUR w porównaniu z 6,5–9,7 mld EUR w Azji i 12,1–18,6 mld EUR w Ameryce Północnej"[35]. B+R oraz pobudzenie innowacyjności ma opierać się także na tworzeniu dedykowanych SI ośrodków badawczych i sieci centrów innowacji cyfrowych oraz wprowadzeniu w życie niezwykle ciekawej inicjatywy: „platformy sztucznej inteligencji na żądanie" pomagającej lepiej wykorzystywać potencjał technologii SI zainteresowanym podmiotom, szczególnie małym i średnim przedsiębiorstwom (MŚP)[36]. Rzeczywiście biorąc pod uwagę rolę MŚP w europejskiej gospodarce, a jednocześnie obserwując, jak słabo wykorzystują one nowe technologie, należy uczynić je obszarem priorytetowego wsparcia. Potwierdzają to dane. W 2017 roku zaledwie 25% dużych przedsiębiorstw w UE oraz 10% MŚP wykorzystywało analitykę dużych zbiorów danych[37]. Niskie jest także wykorzystanie przetwarzania danych w chmurze, a sam rynek dostawców rozwiązań chmurowych jest silnie zdominowany przez pozaeuropejskie przedsiębiorstwa. W globalnym rynku chmury publicznej rozwiązania firmy Amazon stanowią 47,8%, Microsoft Azure 15,5%, Alibaba 7,7%, Google 4% i IBM 1,8%[38]. Brak jest europejskich czempionów, którzy liczyliby się tak na świecie, czy nawet na samym rynku europejskim. W chwili obecnej podejmowane są próby przełamywania praktycznego monopolu pozaeuropejskich dostawców rozwiązań chmurowych. Jedną z nich jest projekt budowy europejskiej infrastruktury chmurowej GAIA-X[39]. To pomysł mający duży potencjał, choć sceptycy wskazują, że aktualna lista podmiotów partycypujących w projekcie nie wskazuje na to, że łatwo uda się osiągnąć paneuropejskie rozwiązania realnie konkurujące z aktualnymi liderami[40]. Niemniej jednak budowa infrastruktury cyfrowej i większego wykorzystania innowacyjnych technologii przez europejskie podmioty jest kluczowa także dla rozwoju SI i musi być wspierana.

Warto zwrócić uwagę na ciekawe działania, jakie podejmuje UE w kolejnym z fundamentalnie ważnych obszarów dla rozwoju SI – dostępie do danych. Dane są paliwem napędowym sztucznej inteligencji. To zasób, który koniecznie należy uwolnić, jeśli UE chce mieć znaczenie w globalnym wyścigu technologicznym. Mając świadomość wagi problemu, Bruksela przygotowuje szereg rozwiązań. W ostatnim czasie ogłoszona została europejska

strategia w zakresie danych[41], która zakłada wprowadzenie mechanizmów sprzyjających otwieraniu i dzieleniu się danymi – ma na celu stworzenie wspólnej europejskiej przestrzeni danych. Z punktu widzenia uwolnienia potencjału Europy i doganiania liderów, jest to konieczne działanie. Nie wiadomo, jaki ostatecznie kształt przyjmą działania UE w tym zakresie ani jak wiele kwestii zostanie silnie uregulowanych. I o ile strategia zachęt i ułatwień związanych z uwalnianiem danych jest kluczowa, nie wiadomo, czy bez czynnika bardziej mobilizującego przyniesie zakładany efekt. Szczególnie, że już teraz widać, że przedsiębiorstwa są niechętne dzielenia się swoimi zasobami[42].

Ambitne plany UE, by mogły zostać zrealizowane, będą potrzebowały dużej determinacji oraz jedności między państwami członkowskimi. Nie będzie to łatwe zadanie. Niemniej jednak warto budować na już osiągniętych sukcesach i pozytywnych sygnałach, których nie brakuje. Już teraz UE buduje przodującą pozycję np. w obszarze robotyki (w tym przemysłowej) – Komisja zainicjowała ważne inicjatywy na rzecz opracowania wydajnych komponentów i systemów elektronicznych, w tym chipów zaprojektowanych do prowadzenia operacji związanych z SI (neuromorficzne układy scalone). Jednym z flagowych projektów w tych obszarach jest the European Processor Initiative. Uruchomiono także inicjatywy na rzecz rozwoju światowej klasy komputerów o dużej mocy obliczeniowej oraz projekty dotyczące technologii kwantowych i mapowania ludzkiego mózgu[43].

Na koniec warto podkreślić, że poza działaniami na poziomie Unii także poszczególne kraje członkowskie inwestują w budowę swoich własnych zasobów.

2.5. NATO

SI zostało wskazane jako największe technologiczne wyzwanie, jakie stoi przed państwami sojuszniczymi[44]. Początek tekstu wyjaśnił, dlaczego SI jest czynnikiem zmieniającym postać środowiska bezpieczeństwa, prowadzenia konfliktów, jak już teraz kształtuje ono pole walki. Sojusz jako organizacja, jak również poszczególni członkowie, będą musieli rozwijać swój potencjał w zakresie pozyskiwania, rozwijania, a przede wszystkim implementacji SI. Będzie to wymagało także niełatwych działań koordynacyjnych, szczególnie związanych z wykorzystaniem systemów opartych na SI w działaniach operacyjnych. Wyzwania natury politycznej, prawnej, związanej z interoperacyjnością przyjętych rozwiązań będą poważnymi wyzwaniami dla NATO. Sojusz musi zdefiniować procesy i standardy weryfikacji, walidacji i akredytacji systemów SI[45]. Oczywiście fundamentalne znaczenie mają kwestie etyczne i związane z bezpieczeństwem.

NATO musi dokonać także głębokich analiz dotyczących możliwości wykorzystania SI do osłabiania przeciwnika w kontekście możliwych konfliktów zbrojnych. Opisane wcześniej zagadnienie obezwładnienia systemów wykorzystywanych do izolacji pola walki opartych o SI może mieć strategiczne znaczenie, także z punktu widzenia bezpieczeństwa krajów Trójmorza.

SYTUACJA GLOBALNA I WNIOSKI DLA REGIONU TRÓJMORZA

Państwa regionu Europy Środkowo-Wschodniej muszą przyjąć własny plan udziału w wyścigu dotyczącym SI. Wynika to zarówno z wcześniej opisanych potrzeb dotyczących bezpieczeństwa, jak i rozwoju gospodarczego. Wedle Komisji Europejskiej na dzień 5 sierpnia 2020 połowa państw Trójmorza ma gotową strategię rozwoju SI, a druga połowa prowadzi zaawansowane prace nad finalizacją dokumentu[46]. Analiza dostępnych dokumentów pokazuje, że poszczególne kraje planują stawiać w dużej mierze m.in. na rozwój edukacji, B+R, niezbędnej infrastruktury cyfrowej, środowiska regulacyjnego (m.in. działania powiązane z kwestiami etyki), przyśpieszenia wdrożeń technologii SI w kluczowych sektorach. Biorąc pod uwagę czynniki, które zadecydują o tym, kto

będzie wiódł prym w wyścigu technologicznym dotyczącym SI, sukces Trójmorza będzie w dużej mierze uzależniony od tego, czy państwa regionu będą w stanie nie tylko samodzielnie rozwijać swój własny potencjał, ale także czy, będąc członkami UE, przyczynią się do rozwoju potencjału całej wspólnoty. UE i jej członkowie będą w stanie konkurować z gigantami takimi jak USA czy Chiny, tylko gdy wspólnie, w sposób zharmonizowany zaadresują kluczowe wyzwania. Uwalnianie danych i dostępu do nich, edukacja, wsparcie biznesu (szczególnie MŚP), rozwój infrastruktury – to niezbędne działania, które muszą być budowane ponadnarodowo. W interesie regionu jest wzmacnianie koncepcji budowy strategicznej autonomii cyfrowej UE. Silna UE, to silne Trójmorze, silne Trójmorze to silniejsza UE. Poza wzmacnianiem potencjału Wspólnoty, państwa regionu powinny jednak promować rozwój cyfrowy we współpracy z partnerami. Autonomia to nie autarkia, niemniej jednak większa niezależność Europy jest konieczna.

Dodatkowo państwa Trójmorza muszą obserwować aktualne trendy geopolityczne, tak aby ich strategiczne decyzje były z nimi zharmonizowane i przynosiły wartość dodaną. Jednym z nich jest promowanie przystępowania do swoistych „nowych technologicznych koalicji", głownie pod przywództwem USA. Decyzje w tym zakresie powinny być uwarunkowane kwestiami bezpieczeństwa, wspieraniem wspólnych wartości, ale także pragmatycznymi rozmowami dotyczących ewentualnych korzyści, jakie mogą płynąć z wspierania poszczególnych inicjatyw. Korzyści te mogą mieć między innymi wymiar wsparcia technologicznego, także w zakresie rozwoju SI, czy też korzystnych decyzji związanych ze zmianami dotyczącymi globalnego łańcucha wartości.

Na koniec warto przypomnieć, że rozwój SI będzie miał nie tylko znaczenie ekonomiczne, ale także obronnościowe. Trójmorze położone jest w newralgicznym obszarze geopolitycznym. Wyżej opisane możliwości wykorzystania SI w wymiarze militarnym i potencjalny wpływ tych działań na strategiczną równowagę w regionie powinien być w centrum uwagi podmiotów odpowiedzialnych za bezpieczeństwo zarówno na poziomie poszczególnych krajów, jak i NATO. Państwa regionu muszą promować konieczność prowadzenia zaawansowanych analiz wykorzystania SI w konfliktach zbrojnych, a także przede wszystkim mobilizować rozwój zdolności w tym zakresie. Szczególnie że państwa takie jak Rosja – stanowiące główne zagrożenie dla regionu – aktywnie włączają technologię SI do swojego arsenału działań.

NIEUCHRONNOŚĆ W NIEPEWNOŚCI

Świat znajduje się aktualnie w okresie wielkiej „niepewności"[47] dotyczącej rozwoju i wykorzystania SI. Niepewne jest także to, którzy gracze będą odgrywali dominującą rolę w zbliżającej się erze SI. Dzisiejsze decyzje i działania tychże aktorów zdeterminują ich przyszłą pozycję geopolityczną. Nie są to słowa przesadzone, bowiem potencjał SI z punktu widzenia ekonomii, a więc bogacenia się państw, ich pozycji w łańcuchu wartości, innowacyjności, ma żywotne znaczenie. Kluczowy będzie także wpływ SI na kwestie związane z bezpieczeństwem. Nie dziwią zatem patetyczne poniekąd stwierdzenia o rządzeniu światem przez dominację w obszarze sztucznej inteligencji. Ostatnie miesiące pokazały dobitnie, że nowoczesne technologie będą nie tylko sercem rywalizacji między wielkimi mocarstwami, ale także obszarem tworzenia się nowych koalicji i sojuszy. Starcie odbędzie się na polu nauki, w obszarze regulacji, współpracy z biznesem, szybszego i bardziej skutecznego wdrażania technologii, a także kształtowania wizji, zasad jej funkcjonowania. Wiele jest za nami okresów „zimy" w zakresie rozwoju SI. I choć nie wiemy jeszcze, jak potoczą się losy jej rozwoju, gdzie są limity, jak duże możliwości, jedno jest pewne. Wyścig napędzany rozwojem SI rozpali świat geopolityki na wiele lat.

PRZYPISY

1 Crow L., *Demis Hassabis on AI's potential*, The Economist, [online:] https://theworldin.economist.com/edition/2020/article/17385/demis-hassabis-ais-potential.

2 Lee K., *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, (Poznań: Media Rodzina, 2019), s. 13-18.

3 *Putin: Leader in artificial intelligence will rule world*, CNBC, 04.09.2017, [online:] https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html.

4 Kohli T., *AI's contribution to the global economy will bypass that of China and India by 2030, to reach $15.7 trillion*, World Economic Forum, [online:] https://www.weforum.org/agenda/2019/09/artificial-intelligence-meets-biotechnology/.

5 Davis Z. S., *Artificial Intelligence on the Battlefield. An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise*, LLNL, 03.2019, s. 7.

6 Davis Z. S., op. cit., s. 7.

7 Kania E. B., *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, Center for a New American Security, 28.11.2017, s. 4.

8 *Interim Report*, National Security Commission on Artificial Intelligence, 11.2019 [za:] 2018 Global R&D Funding Forecast, R&D Magazine, p. 17

9 National Security Commission on Artificial Intelligence, op. cit., s. 17.

10 Kania E. B., op. cit., s. 4.

11 National Security Commission on Artificial Intelligence, op. cit., s. 18.

12 *On the development of artificial intelligence in the Russian Federation*, The President of the Russian Federation, No. 490, 11.10.2019, [online:] http://publication.pravo.gov.ru/Document/View/0001201910110003?index=24&rangeSize=1%3E.

13 Dear K., *Will Russia Rule the World Through AI?*, The RUSI Journal, 11.2019, s. 38

14 Tamże, s. 55.

15 Tamże, s. 57.

16 Tamże, s. 37.

17 Bendett S., Kania E. B., *A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry*, ASPI, Policy brief Report No. 22/2019, 29.10.2019, s. 5.

18 Dear K., op. cit., s. 39-42.

19 *Russian Combat Engineers receive Kapitan UGV*, OVD, 26.07.2019, [online:] https://www.overtdefense.com/2019/07/26/russian-combat-engineers-receive-kapitan-ugv/; Atherton K. D., *New Russian Robot Can Climb Stairs And Blow Up Bombs*, Forbes, 14.05.2019, [online:] https://www.forbes.com/sites/kelseyatherton/2020/05/14/new-russian-robot-can-climb-stairs-and-blow-up-bombs/#515409cd3845.

20 National Security Commission on Artificial Intelligence, op. cit.

21 Tamże, s. 1.

22 Tamże, s. 11.

23 Tamże, s. 20.

24 *Executive Order on Maintaining American Leadership in Artificial Intelligence*, White House, 11.02.2019, [online:] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

25 National Security Commission on Artificial Intelligence, op. cit., s. 21.

26 Tamże, s. 29.

27 *NATO Science & Technology Organization, Science & Technology Trends 2020-2040*, NATO Science & Technology Organization, 03.2020, s. 53.

28 *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, White House, 15.05.2019, [online:] https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

29 *Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China*, NAFSA, 16.06.2020, [online:] https://www.nafsa.org/regulatory-information/proclamation-suspending-entry-chinese-students-and-researchers-connected-prc/.

30 Patrz np. *Sztuczna inteligencja dla Europy*, Komisja Europejska, COM(2018) 237 final, 25.04.2018

31 *White Paper, On Artificial Intelligence - A European approach to excellence and trust*, European Commission, COM(2020) 65 final, 19.02.2020; *The Ethics Guidelines for Trustworthy Artificial Intelligence*, High-Level Expert Group on Artificial Intelligence, 08.04.2019.

32 Świątkowska J., *Projecting power with data*, Directions, 15.05.2019, [online:] https://directionsblog.eu/projecting-power-with-data/.

33 *Sztuczna inteligencja dla Europy*, op. cit., s. 10.

34 Tamże.

35 Tamże, s. 4

36 Tamże.

37 Tamże, s. 5.

38 *Gaia-X, Europe's competitor to Silicon Valley's cloud computing offerings, takes shape*, AADHU, [online:] http://www.aadhu.com/gaia-x-europes-competitor-to-silicon-valleys-cloud-computing-offerings-takes-shape/.

39 Tamże.

40 Dec Ł., *Polska/Europa cybersuwerenna*, TELKO.in, 12.06.2020, [online:] https://www.telko.in/polska-europa-cybersuwerenna.

41 Świątkowska J., *Projecting power with data*, Directions, 15.05.2020, [online:] https://directionsblog.eu/projecting-power-with-data/.

42 Heikkila M., *The Achilles' heel of Europe's AI strategy*, Politico, 13.03.2020, [online:] https://www.politico.eu/article/europe-ai-strategy-weakness/.

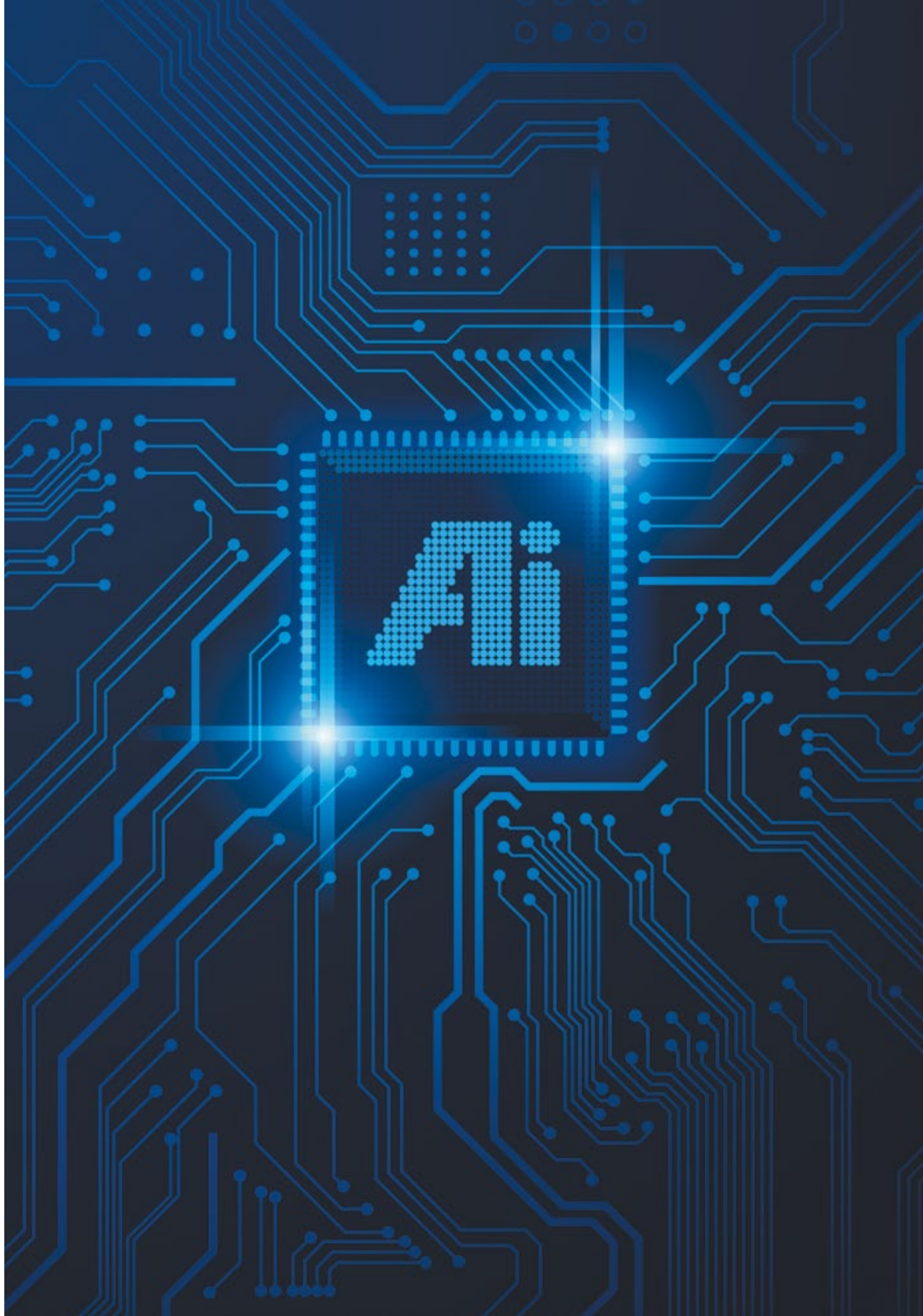
43 *Sztuczna inteligencja dla Europy*, op. cit., s. 6.

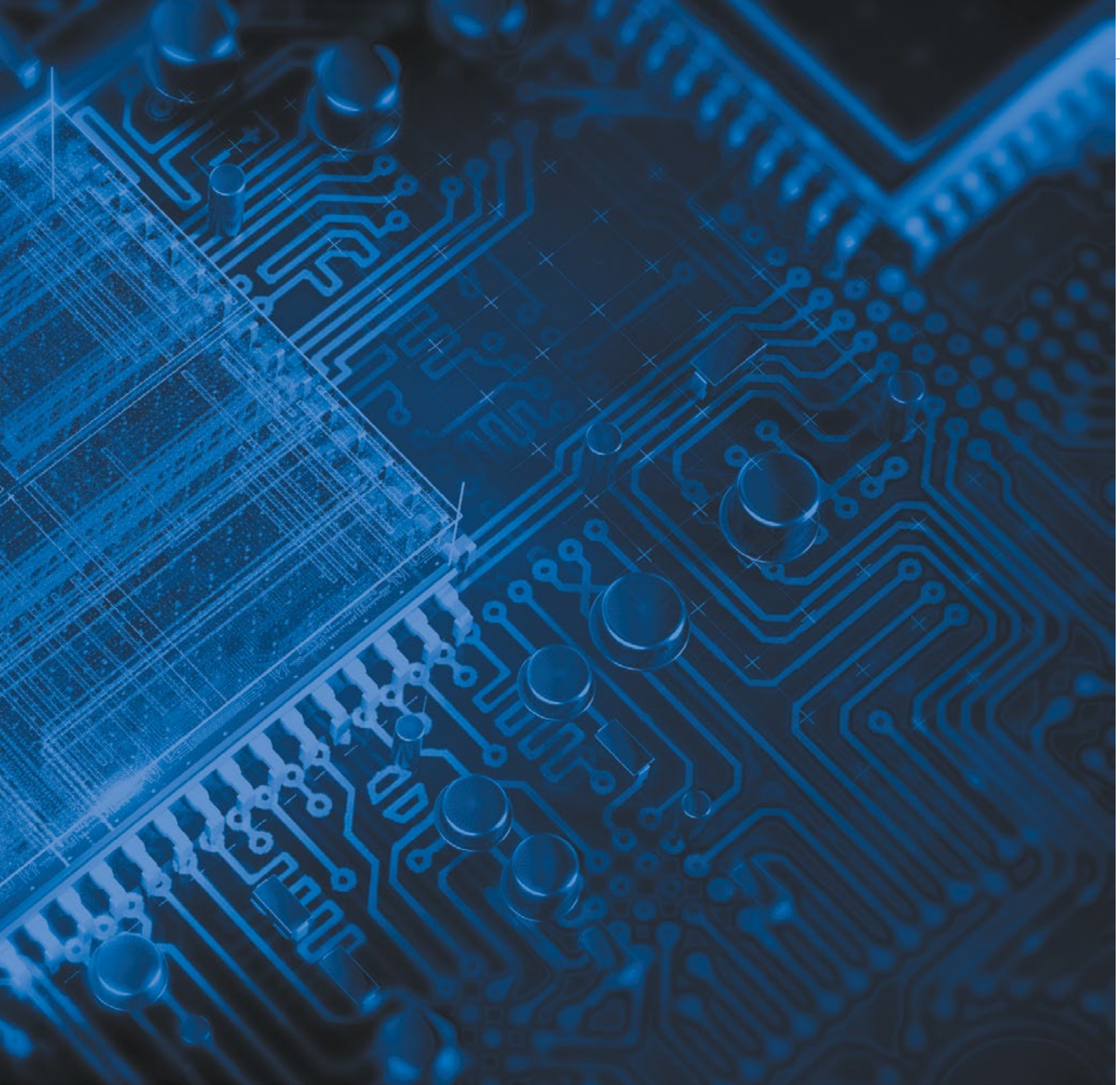
44 NATO Science & Technology Organization, op. cit., s. 50.

45 *NATO Science & Technology Organization, Science & Technology Trends 2020-2040*, s. 57.

46 *Hungary AI Strategy Report*, European Commission, 05.08.2020, [online:] https://ec.europa.eu/knowledge4policy/ai-watch/hungary-ai-strategy-report.

47 National Security Commission on Artificial Intelligence, op. cit. s. 13.





Andrea G. Rodríguez

NA SZLAKU DO KWANTÓW: BEZPIECZEŃSTWO I NASTĘPSTWA GOSPODARCZE INFORMATYKI KWANTOWEJ

W 2016 Unia Europejska opublikowała *Quantum Manifesto* (Manifest kwantowy), wzywając do działań, aby przewodzić drugiej rewolucji kwantowej. Zgodnie z dokumentem, UE rozpoznaje strategiczną wagę technologii kwantowych z racji nie tylko ich potencjalnych następstw w obszarze bezpieczeństwa narodowego, ale też „ulepszeń pod względem możliwości, reaktywności i prędkości, które będą newralgicznym czynnikiem sukcesów w wielu branżach i na wielu rynkach”[1].

Technologie kwantowe to seria wdrożeń informatycznych korzystających z postępów mechaniki kwantowej, która bada materię na poziomie subatomowym, i wykorzystujących niektóre jej zasady dla poprawy wydajności. Ich spodziewanym efektem jest rewolucja w dziedzinach takich jak detekcja i pomiary, obrazowanie, łączność, obliczenia i symulacje, która pozostanie w czołówce innowacji technicznych w nadchodzących latach. Finansowanie badań nad technologiami kwantowymi stało się w wielu krajach i regionach nieodzowne w dążeniu do zrównoważonego rozwoju gospodarczego i przyciągania inwestycji, wkraczania na nowe rynki, rozwoju branży wysokich technologii oraz dbałości o bezpieczeństwo państwowe.

Lista technologii kwantowych jest niemała. Spośród należących do niej kategorii najbardziej obiecujące są jednak zastosowania komunikacji kwantowej i obliczeń kwantowych („informatyka kwantowa” w dalszej części tekstu).

Korzystając z podstawowych zasad mechaniki kwantowej, informatyka kwantowa używa superpozycji i splątania. W komputerach klasycznych bity – podstawowe jednostki informacji – przyjmują wartość 0 lub 1; w obliczeniach kwantowych bity kwantowe (kubity) są w superpozycji. Oznacza to, że mogą przyjmować równocześnie wartości 0, 1 i wszelkie pośrednie[2]. Dodatkowo są niepowtarzalne i nie sposób ich skopiować, dwa lub więcej bity kwantowe mogą jednak zostać ze sobą powiązane i wpływać na swoje zachowanie nawet przy znacznych dystansach. Ta zasada, splątanie, nazwane przez Einsteina „upiornym działaniem na odległość", skutkuje wieloma możliwościami rozwoju bezpiecznych systemów łączności. W połączeniu z superpozycją oba prawidła stanowią fundament nowego paradygmatu obliczeniowego.

NASTĘPSTWA INFORMATYKI KWANTOWEJ DLA BEZPIECZEŃSTWA PAŃSTWOWEGO

Technologie te wpłyną na bezpieczeństwo informacji. Dziedzina ta dokłada starań, by chronić „informacje i systemy informatyczne przed nieautoryzowanym dostępem, użyciem, ujawnieniem, zakłóceniem, modyfikacją czy zniszczeniem, a zapewniać ma poufność, integralność i dostępność"[3]. Szyfrowanie gwarantuje brak jakiejkolwiek modyfikacji (integralność), dostęp stron do informacji (dostępność) oraz znajomość treści wyłącznie przez dopuszczone strony (poufność).

Wśród wad wymienić można zagrożenie dla ochrony danych, które powstaje w wyniku postępu informatyki kwantowej. Komputer kwantowy to urządzenie korzystające z zasad mechaniki kwantowej, by wykonywać operacje na danych. Mimo znaczących postępów w zakresie tzw. wyżarzania kwantowego osiągniętych przez firmy takie jak D-Wave Systems czy procesorów kwantowych IBM i Google'a nadal daleko nam do uniwersalnego komputera kwantowego. Niemniej, skoro zbliżamy się do granic prawa Moore'a, pytanie brzmi nie „czy taka technologia się rozwinie", ale „kiedy" i „jak przeciwdziałać jej negatywnym skutkom".

Te dwa powody – pewność skonstruowania w przyszłości uniwersalnego komputera kwantowego i jego następstwa dla szyfrowania – sprawiają, że podmioty działające w złej wierze będą usiłowały zebrać jak najwięcej informacji. Przy niskich kosztach przechowywania danych wrogie siły mogą je gromadzić, dopóki nie zdobędą dostępu do technologii pozwalającej na odszyfrowanie. Takie gromadzenie danych (*harvesting attacks*) jest szkodliwe zwłaszcza dla krajowych wywiadów, ma wyraźne efekty kaskadowe i już obecnie do niego dochodzi.

Wśród zalet ultranowoczesnej komunikacji kwantowej wymienić zaś można bezpieczne przechowywanie, przesył i przetwarzanie informacji. Przewagą kwantowych czy postkwantowych mechanizmów cyberbezpieczeństwa jest fakt, że są kompatybilne z naszymi istniejącymi sieciami i systemami. Można je więc implementować w klasycznych sieciach, aby zabezpieczały klasyczną komunikację. Wadę stanowi jednak nierozstrzygnięty problem, czy takie mechanizmy uniemożliwiają włamanie uniwersalnym komputerom kwantowym.

Dla zabezpieczenia danych w obliczu nadejścia obliczeń kwantowych amerykański Narodowy Instytut Standardów i Technologii (NIST) podjął inicjatywę standaryzacji postkwantowych algorytmów kryptograficznych, które zastąpią dotychczasowe algorytmy. W czerwcu 2020 roku NIST wciąż oceniał propozycje z drugiej rundy, w której brało udział 26 uczestników[4]. Instytut skupia się na rozwoju algorytmów szyfrujących z kluczem publicznym, ponieważ informatyka kwantowa właśnie na nie wpłynie najpoważniej.

Nie licząc kryptografii postkwantowej, kwantowa dystrybucja klucza (ang. QKD) pozwala stronom komunikować się bezpiecznie nawet w środowisku postkwantowym. Protokoły QKD generują liczby losowe na podstawie entropii, aby przekazać tajny klucz między dwiema stronami w sposób niezwykle bezpieczny[5]. Bezpieczeństwo klucza rośnie przez losowość nieodzowną w mechanice kwantowej. Ponadto, z powodu szczególnych własności kubitów, uczestnicy komunikacji wiedzą, jeśli

atakujący podsłucha klucz, i zatrzymują wymianę informacji, zanim jakiekolwiek ulegną ujawnieniu.

Choć teoretycznie QKD może pomóc w uporaniu się z powstającymi problemami kwantowej przyszłości, zarazem lepiej zabezpieczając dotychczasowe formy komunikacji, przed uczonymi nadal wiele pracy nad rozwiązaniem kwestii dekoherencji (jak długo kubity mogą krążyć, a informacje być przechowywane) i niezawodności komunikacji kwantowej. Obecne kanały dystrybucyjne QKD są mało rozbudowane i zależą od klasycznej infrastruktury.

Na przykład w Europie politechnika w Delft prowadzi projekt mający stworzyć kwantową sieć internetową najpierw do 2022 roku w Holandii[6], a następnie w reszcie Europy we współpracy z Quantum Internet Alliance (Sojuszem Internetu Kwantowego), projektem należącym do programu finansowania badań Horyzont 2020. Początkowo sieć będzie się jednak opierać na klasycznych węzłach, co umożliwi łączność długodystansową. Poza europejską inicjatywą naziemną istnieje też chińska bezprzewodowa kwantowa dystrybucja klucza. W roku 2017 Chinom udało się wystrzelić satelitę kwantowego, Mocjusza, który niedługo później pośredniczył w pierwszej konferencji z dystrybucją QKD między Chińską Akademią Nauk w Pekinie a Austriacką Akademią Nauk w Wiedniu[7].

SZANSE ROZWOJU GOSPODARCZEGO ZE STRONY INFORMATYKI KWANTOWEJ

Komputery kwantowe oprócz sfery bezpieczeństwa państwowego tworzą okazję do wielkiego postępu w innych dziedzinach – finansach, przemyśle, ochronie zdrowia czy logistyce. Ponieważ będą w stanie rozwiązywać skomplikowane problemy optymalizacyjne, znajdą zastosowanie w spersonalizowanych portfoliach lepiej dopasowanych przez firmy do klientów. Na dodatek będą mogły czerpać z lepszych prognoz, sprawiając w ten sposób, że technologia przyda się do wykrywania i zwalczania oszustw, prania pieniędzy i krachów finansowych[8].

Również w badaniach nad nowymi materiałami komputery kwantowe okażą się pomocne, co pozwoli wejść na ścieżkę tworzenia nowych branż i optymalizacji produktów. Optymalizacja i symulacje pozwolą natomiast działającym podmiotom walczyć z problemami łańcuchów dostaw w czasie rzeczywistym[9]. Takie możliwości przydadzą się też w sektorze ochrony zdrowia. Ponieważ mechanika kwantowa operuje na poziomie subatomowym, komputery będą ogromnie pomocne przy modelowaniu i symulacji cząsteczek, co pomoże w opracowywaniu nowych leków. Część tych zastosowań niekoniecznie wymaga uniwersalnego komputera kwantowego. Dlatego też firma konsultingowa McKinsey & Co. ocenia, że do roku 2035 wartość rynku informatyki kwantowej przekroczy bilion dolarów[10].

GEOPOLITYKA INFORMATYKI KWANTOWEJ

Oddziaływanie obliczeń kwantowych na obszar bezpieczeństwa państwowego i szanse dla gospodarek krajowych uczyniły rozwój tej dziedziny strategicznie istotnym. Z perspektywy sektora prywatnego przedsiębiorstwa takie jak szwajcarskie ID Quantique oferują rozwiązania QKD zwiększające bezpieczeństwo komunikacji. Na rynku obliczeń kwantowych dominują zaś firmy kanadyjskie i amerykańskie. Obiecujące rozwiązania komercyjne oferują tacy gracze jak D-Wave i IBM. „Ślepe obliczenia kwantowe" IBM dają publiczny dostęp w chmurze do komputera pięciokubitowego[11], a wyżarzacz kwantowy D-Wave oferuje ulepszone procedury symulacji oparte na zasadach superpozycji i splątania[12].

Na płaszczyźnie sektora publicznego przewodzą natomiast w wyścigu Chiny, Stany Zjednoczone i Unia Europejska, realizując ambitne strategie, aby stworzyć solidną branżę technologii kwantowych. Strategie te zdają sobie sprawę z kluczowego znaczenia informatyki kwantowej dla gospodarki i bezpieczeństwa państwa oraz zawierają szereg celów prowadzących do rozwoju pierwszego uniwersalnego komputera kwantowego. Jak zauważono wyżej, ktokolwiek go zbuduje, będzie w stanie złamać

większość systemów kryptografii i odczytać poufne informacje przeciwników. To przełom, który potencjalnie daje do ręki większe cyfrowe możliwości ofensywne, ale przygotowuje też grunt pod nowe odkrycia wpływające na inne obszary operacji takie jak ląd, morze, powietrze i przestrzeń kosmiczna przez opracowanie na przykład nowych materiałów. Co więcej, strategie kwantowe biorą pod uwagę, jak istotna jest dla zbudowania porządnej branży kwantowej kontrola nad kwantowym łańcuchem dostaw, w którym między innymi podkreśla się rolę nadprzewodników.

Trzynasty Plan Pięcioletni Chińskiej Republiki Ludowej *explicite* nazywa rozwój komunikacji kwantowej „branżą strategiczną”[13], ustanawiając badania nad tym typem komunikacji i obliczeń jako jeden z sześciu celów naukowo-technicznych w perspektywie roku 2030. Ważkim krokiem naprzód było wystrzelenie w 2017 pierwszego satelity kwantowego o nazwie Mocjusz, który umożliwił łączność kwantową na duże odległości[14].

W Europie UE opublikowała w roku 2016 *Manifest kwantowy*, który postawił za cel zajęcie przez ten kontynent „pozycji lidera w krajobrazie przyszłego światowego przemysłu”. Choć dokument ten wyszczególnia cztery grupy zastosowań (łączność, symulacje, detekcja i komputery), wskazuje, że „bezpieczeństwo łączności ma znaczenie strategiczne zarówno dla konsumentów, przedsiębiorstw, jak i rządów”[15]. Zgodnie z *Manifestem* Unia uruchomiła w ramach Horyzontu 2020 (rozszerzanego obecnie do Horyzontu Europa) kwantowy program flagowy – Quantum Flagship, aby rozwinąć branże regionu w obszarach łączności, obliczeń, detekcji i pomiarów, nauk podstawowych oraz symulacji[16].

W USA National Cyber Strategy (Krajowa Strategia Cyberbezpieczeństwa) z roku 2018 dostrzega potencjał zakłóceń, który informatyka kwantowa przynosi na poziomie bezpieczeństwa państwa, a także wskazuje na potrzebę implementacji przez USA rozwiązań odpornych na techniki kwantowe[17]. Dwa miesiące po publikacji strategii USA opublikowały National Quantum Initiative Act (ustawę o krajowej inicjatywie kwantowej), „by przyspieszyć kwantowe prace badawczo-rozwojowe na rzecz bezpieczeństwa gospodarczego i państwowego Stanów Zjednoczonych”[18]. Kraj ten przoduje w omawianej dziedzinie w innowacjach sprzętowych, zaś wyniesienie Mocjusza w 2017 roku na orbitę oraz stanowiące jego pokłosie eksperymenty stawiają Chiny w roli lidera w telekomunikacji kwantowej.

Tymczasem w kontekście NATO spodziewane przez Sojusz skutki są „głębokie i różnorodne”[19]. Z jednej strony oczekuje się, że informatyka kwantowa radykalnie wzmocni NATO pod kątem strategicznym i operacyjnym. Z drugiej jednak strony przyjmuje się, że ulepszenia w dziedzinie komunikacji kwantowej i superbezpieczne kanały łączności rzucą wyzwanie możliwościom systemów dowodzenia (C4ISR) Sojuszu, a główne zagrożenia przyjdą ze strony „konkurentów o zbliżonej sile”[20], którzy potrafią zaktywizować fundusze na potrzeby badań i rozwoju w obszarze informatyki kwantowej.

W JAKIM PUNKCIE JESTEŚMY? GOTOWOŚĆ NA DZIEŃ Q: REGION TRÓJMORZA I POLSKA

NATO ocenia w roku 2020, że pierwszy uniwersalny komputer kwantowy stanie się dostępny około roku 2040, a w ocenie UE nie nastąpi to przed 2035[21]. Takie szacunki odsuwają Dzień Q w czasie o co najmniej 15 lat. Niemniej – wobec pewności jego nadejścia ze strony różnych podmiotów, w tym UE, USA czy Chin, jak również postępów w informatyce i wyżarzaniu ze strony firm prywatnych takich jak D-Wave czy Google – podszyte złymi intencjami działania z gatunku „pobierz teraz, odszyfruj później” już rozpoczęto, zatem czas, by zabezpieczyć łączność i inwestować w technologie kwantowe, już nadszedł.

Na obszarze Trójmorza dostrzec można znakomite okazje inwestycyjne i rozwojowe w zakresie stosowania technik kwantowych. Po pierwsze dysponuje on 22% ludności Europy i 10% PKB kontynentu. Wsparcie ekosystemu innowacji

i doskonalenia w ramach Inicjatywy Trójmorza oraz projektu Quantum Flagship miałoby korzystny wpływ na transformację cyfrową, zarazem pomagając w wyjściu z gospodarczego kryzysu wywołanego przez pandemię COVID-19.

W sektorze kwantowym krakowska firma Beit Tech i warszawska Quantumz.io to główne przykłady polskiej aktywności inwestycyjnej w informatyce kwantowej. Obie skupiają się na oprogramowaniu. Tabela 1 pokazuje najistotniejsze przedsiębiorstwa działające w obszarze informatyki kwantowej w regionie Trójmorza. Już na pierwszy rzut można wyciągnąć dwa wnioski:

- Austria, Estonia i Polska stoją na czele regionalnych wysiłków w informatyce kwantowej, a większość firm poświęca się rozwojowi oprogramowania kwantowego,
- choć potencjał regionu jest wysoki w kwestii zaangażowania w zrównoważony wzrost gospodarczy i sprzyjania za pomocą technologii informatycznych szybkiemu ożywieniu ekonomicznemu po pandemii, firm poświęcających się przygotowywaniu rozwiązań kwantowych nie ma zbyt wiele.

TABELA 1.
NAJWAŻNIEJSZE FIRMY TRÓJMORZA PRZYGOTOWUJĄCE ROZWIĄZANIA Z OBSZARU INFORMATYKI KWANTOWEJ[22].

Kraj pochodzenia	Nazwa przedsiębiorstwa	Specjalność
Austria	Alpine Quantum Technologies GmbH	sprzęt
	ParityQC	sprzęt + programy
Bułgaria	SHYN	programy
Czechy	Quantum Phi	konsulting
Estonia	Ketita Labs	programy
	Quantastica	programy
Polska	Quantumz.io	programy
	Beit Tech	programy

Aby wyzwolić pełnię potencjału drzemiącego w informatyce kwantowej dla dobra gospodarki regionu i zadbania o jego bezpieczeństwo państwowe, wskazane jest:

- Inwestować w rozwiązania bezpieczne w obliczu technologii kwantowych i w przejście do komunikacji kwantowej. Ataki superpozycyjne będą szkodzić nie tylko gospodarce, ale też bezpieczeństwu państwowemu. Korzystanie z protokołów odpornych na ataki kwantowe i szyfrowania przepisującego to taktyka wyprzedzająca, która nie pozwoli napastnikom czerpać korzyści z chomikowania danych. Informacje poufne

z zakresu wywiadu krajowego oraz kluczowe dane o ochronie infrastruktury krytycznej to przykłady stawki w tej grze.

- Sprzyjać współpracy między sektorem publicznym a prywatnym: utrzymujące się inwestycje w obrębie informatyki kwantowej pomogłyby pokierować wysiłkami w regionie. Przy skupieniu się większości firm na oprogramowaniu promocja ekosystemu doskonalenia software'u kwantowego mogłaby przeorientować europejskie starania w tym zakresie na Europę Środkowo-Wschodnią, skupiając europejską strukturę innowacji w bliskiej przyszłości na tym jej uczestniku.

- Przyczyniać się do atmosfery regionalnej współpracy i wymiany pomysłów: dzielenie się doświadczeniami, zachęcanie do wspólnego udziału w projektach Quantum Flagship i bliska współpraca mogłyby pomnożyć pozytywne skutki informatyki kwantowej w regionie 3S.

Podsumowując, choć wizje roztaczane na podstawie informatyki kwantowej są z pozoru rodem z science fiction, przewidzenie rozwoju uniwersalnego komputera kwantowego i łagodzenie zawczasu jego negatywnych skutków to rzecz nieodzowna. Zważywszy na implikacje geopolityczne oraz korzyści gospodarcze, uznanie strategicznej wagi technologii kwantowych może wywołać pozytywne efekty. Gra toczy się o olbrzymią stawkę, wyzwania już istnieją, a Polska i region Trójmorza muszą postanowić, czy odgrywać będą istotną rolę w kolejnym informatycznym przełomie, czy pozwolą się nieść nurtowi czasów.

PRZYPISY

1 *Quantum Manifesto: a New Era of Technology*, Unia Europejska, 05.2016, [online:] https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf.

2 Jaeger L., *The Second Quantum Revolution: from Entanglement to Quantum Computing and Other Super-Technologies*, Cham: Springer, 2018.

3 Barker W. C., *Guideline for Identifying an Information Security as a National Security System*, U.S. Department of Commerce, National Institute of Standards and Technology, 2013, [online:] https://csrc.nist.gov/glossary/term/information_security.

4 *History of PQC Standardization Round 2 Updates*, NIST, 2020, [online:] https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-2/history-pqc-round-2-updates.pdf.

5 Xavier G. B., Ferreira Da Silva T., Vilela da Faria G., Penello Temporão G., Von der Weid J., *Practical random number generation protocol for entanglement-based quantum key distribution*, Quantum Information & Computation 9/2010, s. 683–692.

6 Vermaas P., Nas D., Vandersypen L., Elkouss Coronas D., *Quantum Internet: The Internet's Next Big Step*, Delft: Delft University of Technology, 2019.

7 Ju S., Liu Y., Hu T., *QUESS Operations at Chinese Space Science Mission Centre*, SpaceOps Conference, 2018, doi:10.2514/6.2018-2329.

8 *Innovating with Quantum Computing: Enterprise experimentation provides view into future of computing*, Accenture, 2017.

9 Tamże.

10 Hazan E., Ménard A., Ostojic I., Patel M., *The next tech revolution: quantum computing*, McKinsey & Company, 03.2020, [online:] https://vivatech.cdn.mediactive-network.net/www-site/uploads/2020/04/the-next-tech-revolution-quantum-computing-viva-technology-x-mc-kinsey-company.pdf.

11 *IBM Quantum Experience*, IBM, 2020, [online:] https://quantum-computing.ibm.com/.

12 *Quantum Computer: How D-Wave Systems Work*, D-Wave, 2020, [online:] https://www.dwavesys.com/quantum-computing.

13 *The 13th Five-Year Plan for Economic and Social Development of The People's Republic of China (2016–2020)*, Central Committee of the Communist Party of China, 2016, s. 66, [online:] https://en.ndrc.gov.cn/policyrelease_8233/201612/P020191101482242850325.pdf.

14 Popkin G., *China's Quantum Satellite Achieves 'Spooky Action' at Record Distance*, Science, 15.06.2017, [online:] https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

15 *Quantum Manifesto: a New Era of Technology*, Unia Europejska, op. cit., s. 10.

16 *Strategic Research Agenda*, European Quantum Flagship i Komisja Europejska, 2020.

17 *National Cyber Strategy of the United States of America*, White House, 09.2018, [online:] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

18 *National Quantum Initiative Act*, Kongres USA, 2018.

19 *Science & Technology Trends 2020-2040*, NATO Science & Technology Organization, 03.2020, s. 70, [online:] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

20 Tamże, s. 72.

21 *Quantum Manifesto: a New Era of Technology*, Unia Europejska, op. cit., s. 8.

22 *Private/Startup Companies*, Quantum Computing Report, 2020, [online:] https://quantumcomputingreport.com/privatestartup/.

Kamil Mikulski

ZNACZENIE INFORMACJI W RYWALIZACJI GEOPOLITYCZNEJ

WSTĘP

Informacja, choć wymyka się próbom definicji i jednoznacznej klasyfikacji, jest jednak powszechnie postrzegana jako zasób przydatny w geopolitycznej rywalizacji oraz narzędzie dające przewagę konkurencyjną. Wykorzystanie informacji w relacji zewnętrznej, której adresatami bywają np. podmioty zagraniczne lub środowiska dysydenckie i emigracyjne, przybiera często postacie kampanii dezinformacyjnej, operacji informacyjnej, działań hybrydowych lub propagandy, które z kolei łączone są z pojęciem wojny informacyjnej.

Informacja jako zasób występuje również w aspekcie wewnętrznym[1], w którym państwa usiłują chronić własną cyberprzestrzeń przed obcymi lub konkurencyjnymi wobec rządowych treściami, co przybiera często postać cenzury lub innych form nadzoru nad wewnętrzną przestrzenią informacyjną[a]. W rozpatrywanych przykładach informacja rozumiana jest zatem przede wszystkim jako zorganizowany i celowo stosowany instrument polityki państwowej w stosunkach zewnętrznych oraz wewnętrznych. Celowe wykorzystanie informacji wpisuje się w politykę informacyjną państw, która z kolei służy zabezpieczeniu jego geopolitycznych interesów[2], definiowanych przez rządy i inne podmioty administracji publicznej[b].

a Często również w formie propagandy lub komunikacji strategicznej, które są charakterystyczne dla działań państwa wykorzystujących informacje w relacjach wewnętrznych i zewnętrznych.

b Nie zawsze dotyczy to rządu, mogą być potencjalnie definiowane przez inne podmioty poniżej szczebla rządowego, np. w krajach o zdecentralizowanej władzy wykonawczej.

Geopolityczna rywalizacja między mocarstwami uwidacznia się m.in. w opartej na informacjach cyberprzestrzeni. Wymienione przykłady wykorzystania informacji (np. kampania dezinformacyjna lub cenzura własnej cyberprzestrzeni) związane są często z platformami z sektora mediów społecznościowych, które mają kluczowe znaczenie dla rozprzestrzeniania się informacji online. Postęp technologiczny i upowszechnienie się nowych technologii takich jak *deepfake* czy coraz doskonalsze przetwarzanie języka naturalnego potencjalnie zrewolucjonizują środowisko informacyjne poprzez maszynowe tworzenie treści i mediów. Ułatwi to prawdopodobnie m.in. prowadzenie kampanii dezinformacyjnych, zwiększając ilość i zasięgi fałszywych, ale realistycznie wyglądających treści i mediów. Postęp będzie miał wprawdzie znaczenie globalne, ale szczególnie istotny stanie się w kontekście rywalizacji mocarstw (przede wszystkim Zachodu[c] oraz kwestionujących *status quo* Rosji i Chin).

STRATEGIE DZIAŁAŃ INFORMACYJNYCH MOCARSTW

Rosja

Przypadek rosyjski jest nietypowy z powodu szczególnej wagi, jaką Rosja przydaje informacji w swojej doktrynie. Wojna, prowadzona również środkami niekonwencjonalnymi, stanowi element samopostrzegania i samookreślenia pozycji „ruskiego miru" wobec innych potęg. Przede wszystkim jest zatem narzędziem mającym na celu zarazem ochronę reżimu oraz wywieranie wpływu na państwa trzecie, np. na wybory w USA. Charakterystyczne dla Rosji poczucie zagrożenia z zewnątrz przekłada się na konieczność zagwarantowania bezpieczeństwa poprzez utrzymywanie przeciwników w przekonaniu o sile Rosji i o ich własnej słabości, co w dużej mierze opiera się na wojnie informacyjnej i forsowaniu rosyjskich narracji (np. polityki historycznej). Istotne znaczenie dezinformacji w ramach wojny informacyjnej przypisuje się generałowi Walerijowi Gierasimowowi, którego wykład na temat nowoczesnej rosyjskiej doktryny wojennej (nowa, zmodernizowana *doktryna Gierasimowa*) został wydrukowany 4 marca 2019 r. przez powiązaną z Ministerstwem Obrony gazetę „Krasnaja Zwiezda" pod tytułem *Kierunki rozwoju strategii wojennej*[3].

Wśród widocznych zewnętrznych przejawów wykorzystania (dez)informacji jako narzędzia wyróżnić można działania podejmowane przez służby (GRU, SVR), Agencję Badania Internetu (*Internet Research Agency*, IRA), ale także operację *Secondary Infektion* (zwaną tak na cześć swojej odpowiedniczki z czasów Związku Sowieckiego), czyli operację, która ma na celu rozpowszechnienie wielu różnych narracji dezinformacyjnych w USA i w krajach UE[4]. Co znamienne, w przypadku *Secondary Infektion* ze względu m.in. na bardzo wysoki poziom bezpieczeństwa operacyjnego (ang. OPSEC), trudno jest wskazać, który podmiot jest odpowiedzialny za jej prowadzenie[5]. Warto zwrócić uwagę, że podobnie jak Chiny, Rosja oficjalnie sprzeciwia się ingerencji w swoje sprawy wewnętrzne, a antyrządowe inicjatywy bywają określane jako wroga propaganda lub „dezinformacja". Rosja promuje własne narracje na arenie międzynarodowej i poszukuje sojuszników w różnych kwestiach – to właśnie w kontekście nieingerencji w sprawy wewnętrzne toczono w 2018 r. rosyjsko-hiszpańskie rozmowy na temat utworzenia Wspólnej Grupy ds. Cyberbezpieczeństwa[6], których tłem był kryzys kataloński. Obecnie Rosja posiada największą zdolność (biorąc pod uwagę głównie infrastrukturę i doświadczenie) w zakresie prowadzenia kampanii dezinformacyjnych w państwach trzecich. Moskwa dysponuje wielojęzycznymi mediami (w tym angielskimi, hiszpańskimi, niemieckimi, arabskimi i francuskimi)

c Geopolityczne pojęcie Zachodu jest niedookreślone, w rozumieniu niniejszego artykułu są nim określane przede wszystkim kraje Ameryki Północnej oraz Europy Zachodniej, a także należące do UE/NATO krajów Europy Środkowo-Wschodniej. Ze względu na znaczną fragmentację (kilkadziesiąt państw) poniżej opisane zostaną sumarycznie działania podejmowane na forum międzynarodowym w ramach NATO, a także przez USA oraz UE.

i wykorzystuje je do rozpowszechniania fałszywych i wprowadzających w błąd treści za pomocą m.in. armii botów, trolli oraz ich hybryd[7]. Ponadto Rosja dysponuje rozbudowaną siecią wyspecjalizowanych grup hakerskich przeprowadzających cyberataki i inne działania hybrydowe w cyberprzestrzeni, których metody działania określane są często jako APT[d] (*Advanced Persistent Threats*).

Rosyjska strategia informacyjna skierowana do wewnątrz przybiera dwie istotne formy. Jedną z nich jest przekazywanie społeczeństwu oficjalnej narracji oraz próba wzmacniania poparcia społecznego dla władzy oraz polityki państwa, drugą natomiast jest kontrola oddolnie powstających treści, określana czasem przez władze państwowe jako „walka z propagandą". Dobrym przykładem pierwszego działania jest aktywność tzw. „trolli z Olgino", czyli pracowników IRA, których wewnątrzpaństwowa działalność skupiała się na zwalczaniu opozycji, w tym przede wszystkim Aleksieja Nawalnego, oraz na wychwalaniu rządu[8]. Działalności zewnętrzna i wewnętrzna są, ze względu na swój charakter, często niejawne, stąd wiedzę o operacjach informacyjnych czerpie się z informacji służb (kontr)wywiadowczych, wyspecjalizowanych w wykrywaniu dezinformacji think tanków (np. DFR Lab, Bellingcat), przecieków oraz z wewnętrznych danych publikowanych przez platformy społecznościowe.

Rosyjska polityka informacyjna obejmuje m.in. dążenie do zagwarantowania niezależności i możliwości sprawowania kontroli nad „rosyjskim Internetem", zwanym potocznie RuNetem. RuNet (ros. Рунет) obejmuje głównie strony WWW zarejestrowane pod rosyjskimi (.ru, .su) domenami, ale w szerszym znaczeniu może dotyczyć również rosyjskojęzycznych stron innych krajów regionu. Legislacyjna intensyfikacja „ochrony czystości" RuNetu nastąpiła już w 2016 r. Zgodnie z raportem Rady Europy[9] na operatorów sieci nałożone zostały obowiązki monitorowania i filtrowania treści, w tym przede wszystkim zwalczania m.in. ekstremizmu, propagandy oraz zniesławień. W kompetencje kontrolne wyposażona została Federalna Służba Nadzoru Komunikacji, Technologii Informacyjnych i Mediów (*Roskomnadzor*). Rząd Rosji usiłuje kontrolować RuNet także poprzez ustawę federalną nr 90-ФЗ z 01.05.2019[10], zmieniającą ustawy regulujące komunikację i bezpieczeństwo informacyjne. Nowe prawo o stabilnym RuNecie cechuje się daleko posuniętą autarkią, która dobrze odzwierciedla rosyjską wizję znaczenia informacji i kontroli nad nią (ale także nad danymi, co omówione zostało w rozdziale piątym) w najbliższych latach. Zwiększono kompetencje kontrolne Roskomnadzoru, RuNet *de facto* uznano za infrastrukturę o znaczeniu krytycznym dla państwa, a w rosyjskich firmach telekomunikacyjnych – włączając rosyjskie giganty takie jak Yandex – najwyżej 20% kapitału będzie mogło znajdować się w zagranicznych rękach[11]. Uzupełnieniem walki z wewnętrzną dezinformacją jest nowelizacja art. 207 Kodeksu karnego z maja 2020 r., w myśl której celowe rozpowszechnianie fałszywych informacji zagrożone jest wysoką karą grzywny (do 200 tys. rubli) lub ograniczenia wolności[12]. Nowe prawo spotkało się z negatywną recepcją i oskarżeniem o cenzurowanie niewygodnych dziennikarzy w Rosji[13].

Oprócz zwiększenia bezpośredniej oraz pośredniej ingerencji rządu w wewnętrzną przestrzeń informacyjną Rosji w trend „odzyskiwania kontroli" nad RuNetem wpisują się jeszcze dwie inicjatywy – stworzenie publicznych baz danych dotyczących *fake news* (jedna prowadzona przez MSZ[14] oraz jedna zapowiedziana[15]) oraz obowiązek przechowywania danych dotyczących obywateli Rosji na serwerach zlokalizowanych na terenie kraju[16] (z tego powodu dostęp do rynku rosyjskiego stracił

d Do znanych aktywnych rosyjskich APT należą obecnie: APT 28, APT 29, TeamSpy Crew, TeleBots, TEMP.Veles, Turla (inaczej Waterbug), Blackfly, Wicked Panda, Grim Spider, Lunar Spider, Pinchy Spider, Dragonfly 2.0, Buhtrap, Cobalt Group (Cobalt Spider), Corkow (Metel), Wizard Spider, Zombie Spider, Energetic Bear (Dragonfly), FIN7, Gamaredon Group, Inception Framework, Lurk, MoneyTaker, Operation BugDrop, Roaming Tiger, RTM oraz Iron Viking (inna nazwa Voodoo Bear). Za: *Chinese-speaking hackers increase activity and diversify cyberattack methods*, Techradar.pro, 2020, [online:] https://www.techradar.com/news/chinese-speaking-hackers-increase-activity-and-diversify-cyberattack-methods.

LinkedIn, chociaż miało to miejsce jeszcze na mocy przepisów poprzedniej ustawy z 2014 r.). Zmiany legislacyjne są znacznie szersze i obejmują nawet kilkadziesiąt aktów prawnych, jednak te przytoczone powyżej dobrze oddają kierunek trendu i krytyczne dla Rosji znaczenie panowania nad pieczołowicie budowaną własną cyberprzestrzenią.

Chiny

Zewnętrzna chińska strategia informacyjna przejawia się w rządowych akcjach informacyjnych, gloryfikowaniu ChRL za granicą, a także próbach narzucenia na szczeblu dyplomatycznym własnych narracji (próby zrzucenia z Chin odpowiedzialności za rozprzestrzenienie SARS-CoV-2, próby obarczenia winą Amerykanów[17] oraz Francuzów[18]). Drugim filarem jest koncepcja wojny informacyjnej, która w Chinach ma znaczenie *stricte* militarne i jest elementem doktryny wojennej Chińskiej Armii Ludowo-Wyzwoleńczej, natomiast trzecim – prochińskie grupy wewnątrz państw zachodnich. Z tej trójcy z urzeczywistnianiem chińskiej racji stanu oraz wspieraniem ChRL w rywalizacji geopolitycznej najbardziej związany jest filar dyplomatyczny. To przez działania rządu do innych państw świata przenika chińska dyplomacja publiczna i kulturalna (m.in. Instytuty Konfucjusza[19]). W latach poprzedzających infodemię poświęcono wiele uwagi specyfice „miękkiej" w wyrazie chińskiej wizji narracyjnej, promującej multilateralny porządek świata, nieingerencję w wewnętrzne sprawy państwowe, harmonię, pokój oraz współpracę gospodarczą i technologiczną między krajami. Zyskała sobie ona znaczące miano *dyplomacji pandowej* (od ofiarowanych ogrodom zoologicznym na całym świecie pand – symbolu Chin), tudzież chińskiej *ofensywy uroku* (ang. *charm offensive*). Począwszy od zaostrzenia kursu przez USA w 2018 r. uwidacznia się częściowa zmiana oblicza chińskiej dyplomacji – wojna handlowa, ofensywna retoryka w czasach epidemii COVID-19 oraz incydenty graniczne z Indiami mocno kontrastują z dotychczasowym modelem. Nowa chińska dyplomacja jest bardziej agresywna, asertywna i pewna siebie niż dotychczasowa, co określane bywa jako *wolf-warrior diplomacy*[20]. Państwo Środka promuje własne narracje w skali globalnej, czego przykładem np. wspomniana wcześniej sugestia rzecznika chińskiego MSZ o możliwej odpowiedzialności USA za wybuch pandemii COVID-19[21]. Świadczą o tym również doniesienia Europejskiej Służby Działań Zewnętrznych na temat forsowania narracji ofiarnych Chin, które pełną poświęceń walką z pandemią „kupują czas" dla reszty świata[22]. Narzucane narracje mają na celu ochronę wizerunku ChRL, co odbywa się również dzięki życzliwej postawie Rosji, która na łamach agencji prasowej RIA Novosti broniła Państwa Środka przed międzynarodową krytyką działań państwa podejmowanych w związku z COVID-19[23].

W sferze wewnętrznej zaobserwowano próby kontroli środowiska informacyjnego. Intensyfikacja walki z niepochodzącymi od rządu informacjami (w propagandzie wewnętrznej zwanych często „plotkami") online rozpoczęła się za kadencji obecnego przewodniczącego KPCh, Xi Jinpinga. W polityce wewnętrznej rząd ChRL za pośrednictwem Krajowego Biura Informacji Internetowej (KBII)[24] cenzuruje treści i stosuje umiarkowane środki karne wobec sprawców (z reguły zatrzymania) za naruszenie porządku publicznego[25]. KBII kontroluje głównie strony internetowe, mikroblogi oraz grupy na platformie WeChat. Prawo o Cyberbezpieczeństwie[26] z 2016 r. zwiększa kontrolę nad lokalizowaniem danych oraz nakłada na operatorów sieci, rozumianych jako właściciele, zarządzający lub dostawcy sieci, obowiązek kontroli treści i udostępniania rządowi danych sprawców naruszeń[27]. Prawo o Cyberbezpieczeństwie jest logiczną konsekwencją autarkicznego chińskiego projektu znanego jako Wielki Firewall, który obejmuje m.in. chroniony przed nieautoryzowanymi treściami i zewnętrznymi wpływami własny Internet. Poprzez operatorów bądź samodzielnie rząd definiuje, które niechińskie firmy z sektora mediów społecznościowych mogą operować na rynku oraz reguluje zamieszczane na nich treści zarówno za pomocą cenzury prewencyjnej, jak

i następczej. Kontrolę rządową uzupełniają dwie internetowe „armie" składające się z prorządowych trolli.

Grupy wspierające bądź realizujące wprost politykę władz dzielą się na kilka podstawowych typów:

a. „najemna" „armia 50 centów" (五毛党). Tym pejoratywnym mianem określa się zastępy internautów publikujących prorządowe treści, jak głosi plotka – odpłatnie. W badaniu przeprowadzonym przez zespół naukowców (Gary King i in., 2017) nie znaleziono jej potwierdzenia. Co więcej, badane próby wskazywały na to, że szeregi *wumao dang* zasilali pracownicy administracji rządowej[28].
b. „ochotnicza" „armia 50 centów" (自带干粮的五毛)[29], czyli zróżnicowany, prawdopodobnie przynajmniej częściowo oddolny, ruch prorządowy. Celem „ochotniczej" armii jest walka z prozachodnimi narracjami rozprzestrzenianymi przez „amerykańską centową armię".

Niektórzy badacze wyróżniają także inne odłamy, jednak nie precyzują ich wzajemnej klasyfikacji i relacji względem „ochotniczej armii". Do przykładów należą:

c. „małe czerwone kwiaty" (King G, 2016) będące frakcją czerwonej gwardii[30].
d. „internetowa armia wodna" (King G., 2017) – prorządowe grupy astroturferów[31].
e. grupa „internetowych patriotów" (Han R., 2015), która określa siebie częściej jako „mali różowi" (ze względu na różowy kolor popularnego forum nacjonalistyczno-militarnego[32]),
f. młodzieżówkę KPCh[33] jako samodzielną siłę w aspekcie wewnętrznym.

„Ochotnicza armia" i funkcjonalnie powiązane z nią grupy charakteryzują się działalnością wymierzoną w przeciwników rządu i monitorującą Internet. Pomaga im w tym m.in. zintegrowana baza danych, w której można zgłosić przypadki „plotek"[34].

Wpływ technologii na rozwój dezinformacji

Amerykański think tank Brookings już w 2018 r. ostrzegał, że sztuczna inteligencja może wielokrotnie zwiększyć rosyjski potencjał działań hybrydowych w cyberprzestrzeni[35], a wykorzystanie treści tworzonych przez IRA w ramach prowadzonego przez OpenAI projektu GPT-2 (i następcy, GPT-3) umożliwiło maszynowe generowanie podobnych treści i zarazem potwierdziło, że bliska jest techniczna możliwość automatyzacji dezinformacji i propagandy[36].

Wykorzystanie maszynowego generowania i rozpowszechniania treści należy do zagrożeń nowego typu[37] obok pojawiania się nowych aktorów, decentralizacji oraz rozwoju nowych taktyk w ramach operacji informacyjnych. Przykładowo, jak donosi „New York Times", Rosja rozszerza geograficzny zakres swoich operacji informacyjnych i jest aktywna m.in. w Afryce[38]. Zagrożeniem stają się również automatycznie generowane obrazy, co zostało zaobserwowane m.in. 13 sierpnia 2020, gdy Chiny wykorzystały SI do stworzenia obrazów służących do krytyki aktualnie urzędującego prezydenta USA Donalda Trumpa i wspierania jego rywala w najbliższych wyborach, Joe'a Bidena[39]. Do nowych zagrożeń należy zaliczyć również automatyczną generację obrazu oraz jeden z rezultatów uczenia maszynowego – *deepfake*, czyli fałszywe video stworzone z zastosowaniem technologii *Generative Adversarial Networks* (GANs) symulujące np. wystąpienie polityka.

Trafnym przykładem, jakie konsekwencje może mieć wykorzystanie *deepfake*, jest wielokrotnie przywoływane w literaturze wideo[e], w którym amerykański komik i reżyser Jordan Peele podszył się

e https://www.youtube.com/watch?v=cQ54GDm1eL0

pod byłego prezydenta USA, Baracka Obamę[40]. Na nagraniu widać, jak łudząco podobna do Baracka Obamy postać wygłasza kilka zaskakujących stwierdzeń, w tym inwektywę w stronę aktualnie urzędującego prezydenta Stanów Zjednoczonych, Donalda Trumpa. Opublikowane przez serwis BuzzFeed nagranie skończyło się ujawnieniem, że było w gruncie rzeczy fałszywką i żartem Peele'a, jednak zawierało również ostrzeżenie – demonstrację, w jaki sposób można złośliwie użyć *deepfakes*. Jest to szczególnie niebezpieczne, gdy coraz bardziej popularne stają się aplikacje do manipulacji obrazem, np. przy użyciu chińskiej *Zao*[41] lub rosyjskiej *FaceApp*[42]. Oznacza to, że wymagająca specjalistycznej wiedzy technologia upowszechnia się i za pośrednictwem aplikacji staje się łatwiejsza w wykorzystaniu. Nieszkodliwe programy do obróbki zdjęć i filmów mogą potencjalnie być wykorzystane w przyszłości do innych celów, w tym jako narzędzia wojny informacyjnej.

Współpraca rosyjsko-chińska a wojna informacyjna

Osobnym zagadnieniem pozostaje kwestia współpracy Rosji i Chin, również w dziedzinie wojny informacyjnej. Geostrategiczne interesy tych krajów skutkują kwestionowaniem przez nie istniejącego ładu światowego, zbliżając do siebie obydwa mocarstwa. W 2014 r.[43] odnowiona została strategiczna współpraca między nimi (choć niektórzy autorzy piszą złośliwie o Rosji jako o *junior partnerze*[44] Chin ze względu na rosnącą polityczno-gospodarczą przewagę Państwa Środka). Niezależnie od dynamiki siły, Rosja widzi w Chinach sojusznika m.in. w forsowaniu własnej polityki historycznej[45], natomiast Chiny korzystają z taktyk i doświadczeń rosyjskich w prowadzeniu informacji operacyjnych przeciw Zachodowi (więcej w podrozdziale dot. ChRL). Wspólne kwestionowanie hegemonii Zachodu oraz istniejącego ładu międzynarodowego nie oznacza jednak, że w wymiarze politycznym cele Moskwy i Pekinu są zawsze zbieżne – choćby na odcinku amerykańskim, jak donosi dyrektor NCSC (the US National Counterintelligence and Security Center) William Evanina, Rosja wspiera ubiegającego się o reelekcję Donalda Trumpa, natomiast Chiny i Iran opowiadają się za Joe Bidenem[46]. Chiński potencjał w obszarze operacji informacyjnych przejawia się również w największej na świecie liczbie znanych aktywnych APT[f].

Strategiczna współpraca Rosji i Chin umożliwia Państwu Środka adaptację do swoich potrzeb zaawansowanych taktyk wykorzystywanych przez Moskwę do prowadzenia kampanii dezinformacyjnych. Przejawia się to m.in. w stworzeniu sieci trolli i botów porównywalnych z rosyjskimi, toczeniu wojny informacyjnej (np. promowaniu teorii spiskowych) w cyberprzestrzeni USA, ale również korzystaniu z rosyjskiej infrastruktury informacyjnej, w tym np. Sputnika i RT[47]. Adaptacja ta dotyczy przede wszystkich elementów technologicznych i operacyjnych, a nie samych narracji[48]. ChRL zwiększa swoją obecność i wzmaga działania operacyjne na nowych platformach, testuje taktyki oraz inwestuje w rozwój sztucznej inteligencji, konkurując z USA[49]. Przykładowo, w styczniu 2020 r. Chiny użyły SI do wygenerowania znacznej ilości fałszywych treści, naruszając cyberprzestrzeń Tajwanu[50] w związku z odbywającymi się tam wyborami prezydenckimi.

Gwałtownie zwiększające się możliwości technologiczne Pekinu w prowadzeniu operacji informacyjnych mogą spowodować, że owocami strategicznego partnerstwa z Moskwą będą m.in.:

f Do aktywnych chińskich APT można zaliczyć: APT 1, APT 2, APT 3, APT 4, APT 5, APT 6, APT 9, APT 10, APT 12, APT 14, APT 15, APT 16, APT 17, APT 18, APT 19, APT 20, APT 21, APT 22, APT 23, APT 26, APT 27, APT 30, APT 31, APT 40, Group 72 (inna nazwa: Axiom), Barium, Blackgear, Blue Termite (Cloudy Omega), Bronze Butler (Tick), DragonOK, Elderwood (Sneaky Panda), GhostNet (Snooping Dragon), CactusPete, Goblin Panda (Cycldek), Hidden Lynx (Aurora Panda), Lead, Lotus Blossom (Spring Dragon), Lucky Cat, Moafee, Mofang, Mustang Panda, Naikon (Lotus Panda), Night Dragon, Nitro (Covert Grove), PassCV, PittyTiger (Pitty Panda), Platinum, Rancor, Scarlet Mimic, Shadow Network, Snake Wine, Suckfly, TA459, Taidoor, Temper Panda, Thrip, Blackfly (Wicked Panda), Pacha Group, Rocke. Za: N. K. Cherrayil, *Chinese-speaking hackers increase activity and diversify cyberattack methods*, Techradar.pro, 2020, [online:] https://www.techradar.com/news/chinese-speaking-hackers-increase-activity-and-diversify-cyberattack-methods.

a) pogłębienie koordynacji dyplomatycznej, b) dzielenie przeciwników (*divide et impera*), c) nasilające się korzystanie ze wzajemnej infrastruktury informacyjnej, d) koordynacja nacisków międzynarodowych, e) wspólne wykorzystanie nowych technologii pomocnych w wojnie informacyjnej oraz f) przejęcie globalnych narracji informacyjnych[51]. Przyszłość harmonijnej współpracy rosyjsko-chińskiej nie jest jednak przesądzona – o ile nie ulega wątpliwości, że oba mocarstwa korzystają technologicznie na partnerstwie, pojawiają się prognozy strategicznej kolizji na obszarze znajdującej się w rosyjskiej strefie wpływów Azji Centralnej, gdzie powoli rosną wpływy Chin[52].

WSPÓLNOTA TRANSATLANTYCKA

Wolność słowa i swobody polityczne i społeczne stanowią fundament systemu demokracji liberalnych charakterystycznych dla USA/UE. Do przejawów zewnętrznej działalności USA/UE można zaliczyć globalną promocję zachodniego („uniwersalnego") systemu wartości oraz modelu politycznego, gospodarczego i społecznego. Uniwersalny system wartości rozpowszechniany i promowany jest za pomocą kanałów takich jak media społecznościowe, portale informacyjne lub rozgłośnie radiowe. W aspekcie wewnętrznym Zachód usiłuje chronić własną cyberprzestrzeń przed zewnętrznymi zagrożeniami, np. wypracowując wysokie standardy bezpieczeństwa dla sieci piątej generacji. Za przykład posłużyć tu mogą tzw. *Praskie propozycje* z 2019[53] r. oraz inicjatywa administracji Trumpa Clean Network[54] z 2020 r., zmierzające m.in. do zwiększenia ochrony przed cyberprzestępczością i ochrony danych.

Wyraźną cezurą są wybory prezydenckie w USA w 2016 r. oraz ich następstwo w postaci raportu Muellera, który opublikowano w 2019 r., a Specjalny Radca Robert S. Mueller ujawnił skalę zaangażowania obcych rządów usiłujących wpłynąć na wyniki wyborów w USA[55]. Analiza ta zawierała wiele przykładów nadużyć, w tym nieautentycznych zachowań (ang. *inauthentic behaviours*) charakterystycznych dla botów. Ingerencja została następnie przypisana Rosji i jej agencji IRA, a wkrótce potem podobne incydenty o różnej proweniencji zostały zidentyfikowane i zbadane podczas wyborów lub wydarzeń politycznych (Włochy, Wielka Brytania)[56]. Wzmożenie operacji dezinformacyjnych zauważono także w Unii Europejskiej, np. Wspólne Centrum Badawcze Komisji Europejskiej obserwuje nasilone głoszenie dezinformacji i fałszywych informacji w Internecie, łącząc je ze wzrostem popularności mediów społecznościowych[57]. Prowadzenie zorganizowanych kampanii dezinformacyjnych przypisuje się najczęściej podmiotom działającym z terytorium Rosji, Chin, Iranu i Korei Północnej[58].

Po stronie europejskiej warto wspomnieć o raporcie Europejskiej Służby Działań Zewnętrznych (ESDZ)[59] z 2020 r., opisującym zaobserwowane w państwach członkowskich skoordynowane kampanie dezinformacyjne, użyte taktyki oraz próby przypisania winy za wybuch pandemii COVID-19. Zaznaczyć należy, że postawa UE wobec kampanii dezinformacyjnych stale się usztywnia i podejmowane są kolejne kroki dotyczące zwiększania jej możliwości oraz koordynacji działań państw członkowskich w zakresie zastrzeżonych dla nich kompetencji. Dobrym przykładem jest utworzenie Hybrid Fusion Cell w ESDZ po roku 2016 oraz próby wypracowania wspólnego stanowiska co do zwalczania dezinformacji w drodze unijnego Planu Działania Przeciwko Dezinformacji[60] (2018), a także uchwalenia Kodeksu postępowania w zakresie zwalczania dezinformacji[61] (2018).

MIEJSCE POLSKI I REGIONU TRÓJMORZA W GLOBALNEJ RYWALIZACJI INFORMACYJNEJ

Polska

Operacje informacyjne (zwłaszcza rosyjskie) są prowadzone w Polsce od dawna. Spośród ponad dziewięciu tysięcy przypadków dezinformacji zarejestrowanych przez EUvsDisinfo ponad 250 opublikowano w języku polskim. Do znanych

operacji należą m.in. sugestia z 2015 r., jakoby Polska chciała przyłączyć zachodnią Ukrainę[62], sfałszowane wywiady generałów[63] przed szczytem NATO w 2016 r., zhakowanie przez rosyjskie służby w 2019 r. strony Akademii Sztuki Wojennej i zamieszczenie na niej sfabrykowanego listu rektora Ryszarda Parafianowicza[64] oraz oskarżenie Polski przez białoruskie władze Państwa Związkowego Rosji i Białorusi w sierpniu 2020 r. o zamiar naruszenia integralności terytorialnej państwa w postaci przyłączenia grodzieńszczyzny[65].

Nie ulega wątpliwości, że Polska wielokrotnie bywała celem operacji informacyjnych i rosyjskiej propagandy. Jednocześnie warto zwrócić uwagę na polską specyfikę lokalną, którą tworzą brak licznej mniejszości rosyjskiej, brak popularnych rosyjskich mediów oraz brak większych grup społecznych potencjalnie wrażliwych na dezinformację[66]. W efekcie, Polska jako cel dezinformacji wymusza na jej nadawcy subtelniejszą politykę informacyjną, pozostając rzecz jasna podatna na operacje informacyjne podobnie jak inne kraje regionu.

Zwiększenie odporności Polski na zautomatyzowaną propagandę i operacje informacyjne wymaga zarówno rozwoju własnych zdolności, jak i ścisłej kooperacji z sojusznikami. Obecnie w ramach sektora prywatnego rozwijane są różne inicjatywy monitorujące i przeciwdziałające zautomatyzowanej dezinformacji, m.in. wykorzystująca sztuczną inteligencję ABT Shield[g], czy monitorujący przy pomocy SI treści zamieszczane w portalach społecznościowych Samurai Labs[h]. W zakresie współpracy międzynarodowej Polska angażuje się w działania przeciwko dezinformacji podejmowane przez NATO i UE oraz bilateralnie, przykładowo ratyfikując w 2018 r. polsko-brytyjski Traktat o Współpracy w Dziedzinie Obronności i Bezpieczeństwa[67] oraz prowadząc dialog z USA w zakresie dwustronnej współpracy na rzecz cyberbezpieczeństwa i przeciwdziałania dezinformacji, o czym świadczy spotkanie sekretarza stanu USA Mike'a Pompeo z MSZ Polski Jackiem Czaputowiczem w Warszawie w sierpniu 2020 r.[68].

3SI

Region Trójmorza

Region Trójmorza (3SI), z jednej strony wpleciony w struktury bezpieczeństwa Zachodu, z drugiej historycznie związany z rosyjską strefą wpływów (w tym poprzez RWPG oraz Układ Warszawski) oraz będący przedmiotem polityczno-gospodarczego zainteresowania ChRL (m.in. poprzez inicjatywę 17+1) jest szczególnie narażony na operacje informacyjne, kampanie dezinformacyjne i działania hybrydowe. Dotyczy to jednak zdecydowanie bardziej jego krajów niż 3SI jako koncepcji – sama Inicjatywa stosunkowo rzadko bywa dzisiaj przedmiotem dezinformacji (do wyjątków należą przypadki narracji zaobserwowanych przez EUvsDisinfo głoszących, że 3SI jest inicjatywą antyrosyjską[69] oraz proamerykańską[70] – obie skierowane do polskich internautów). Kraje Inicjatywy Trójmorza posiadają własne specyfiki i podatności, w związku z czym wymierzone są w nie zindywidualizowane kampanie (dez)informacyjne, jak np. związane z kryzysem migracyjnym na Węgrzech, mniejszościami w Estonii czy przedstawianiem Litwy jako kraju słabego i niewartego obrony sojuszniczej[71].

W odpowiedzi na rosnące zagrożenie dezinformacją, w krajach regionu Trójmorza zaczęły pojawiać się technologicznie zaawansowane środki przeciwdziałania fałszywym treściom. Na uwagę zasługuje tu m.in. czeska firma Semantic Visions, która w 2019 r. zwyciężyła amerykańsko-brytyjski Tech Challenge, oferując produkt monitorujący w czasie rzeczywistym newsy online pod kątem dezinformacji[72]. Na osobne wyróżnienie zasłużyła bułgarska Sensika, również monitorująca globalne media ze szczególnym uwzględnieniem języków Azji Mniejszej i Bliskiego Wschodu[73]. Innymi przykładami z regionu są stworzony do przeciwdziałania *deepfake* estoński Sentinel[i], wykorzystująca SI

g https://abtshield.com/

h https://www.samurailabs.ai/

i https://thesentinel.ai/

litewska sieć Debunk (demaskuok[j]), wykorzystujący zautomatyzowany OSINT oraz SI do analizy krzyżowej mediów społecznościowych austriacki SAIL LABS[k] (koordynował projekt Truthcheck w ramach programu Horyzont 2020), a także kolejny bułgarski czempion Ontotext[l] (koordynuje używający uczenia maszynowego projekt WeVerify[m]).

REKOMENDACJE DLA POLSKI DLA KRAJÓW REGIONU TRÓJMORZA

- W celu maksymalizacji własnego bezpieczeństwa i odporności na operacje informacyjne, kampanie dezinformacyjne i działania hybrydowe zarówno Polska, jak i region Trójmorza powinny kontynuować możliwie ścisłą współpracę w ramach transatlantyckich struktur bezpieczeństwa, w tym z ciałami UE (np. Hybrid Fusion Cell, EUROPOL, CERT-EU) oraz NATO (np. NATO StratCom Centre of Excellence).
- Zaproponowana przez Instytut Kościuszki Inicjatywa Cyfrowego Trójmorza stawia sobie za cel zwiększenie bezpieczeństwa regionu w zakresie wspólnych cyberzagrożeń, włączając w to dezinformację[74]. Rozszerzenie Inicjatywy Trójmorza o komponent wymiany informacji oraz współpracy na rzecz przeciwdziałania cyberatakom i operacjom informacyjnym dodatnio przełożyłoby się na bezpieczeństwo regionu.
- Dużą wagę ma obserwacja dynamiki rozwoju technologii i operacji informacyjnych, a także stosowanych przez obce mocarstwa taktyk i narracji.
- Konieczne jest zwiększanie świadomości przedstawicieli sektora publicznego, dziennikarzy i obywateli na temat zagrożeń.
- W przypadku kosztownych i ryzykownych narodowych projektów z zakresu cyberbezpieczeństwa, szczególnie związanych z wdrażaniem nowych technologii, korzystne mogłoby być rozwijanie ich we współpracy z partnerami zagranicznymi z zamiarem współdzielenia kosztów, łączenia zasobów i wymiany *know-how*.
- Zarówno Polska, jak i kraje 3SI powinny ponadto zainwestować w rozwój centrów obserwacji i analizy dezinformacji w mediach społecznościowych, rozwijać technologie, które mają potencjał zwiększenia odporności na operacje informacyjne, w tym przede wszystkim uczenie maszynowe, sztuczną inteligencję, informatykę kwantową, blockchain i *Big Data*.

j https://debunk.eu/about-debunk/

k https://www.sail-labs.com/

l https://www.ontotext.com/

m https://weverify.eu/

PRZYPISY

1 Rosenbach E., Mansted K., *The Geopolitics of Information*, Belfer Center, 2019, s. 8, [online:] https://www.belfercenter.org/sites/default/files/2019-08/GeopoliticsInformation.pdf.

2 Zenko C., *Geopolitical Information Blockades: A New Norm?*, Council on Foreign Relations, 2017, [online:] https://www.cfr.org/blog/geopolitical-information-blockades-new-norm.

3 *Векторы развития военной стратегии*, Krasnaja Zwiezda, 2019, [online:] http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

4 Aleksiejewa N. i in., *Operation "Secondary Infektion". A Suspected Russian Intelligence Operation Targeting Europe And The United States*, Atlantic Council, 2019, s. 6, [online]: https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf.

5 Nimmo C. F., C. S. Eib, L. Ronzaud, R. Ferreira, C. Hernon, T. Kostelancik, *Exposing Secondary Infektion*, Grafika, 2020, s. 11, [online:] https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf.

6 *Russia and Spain Agree to Cooperate on Cyber Security, Fight Fake News*, „The Moscow Times", 2018, [online:] https://www.themoscowtimes.com/2018/11/07/russia-and-spain-agree-to-cooperate-on-cyber-security-fight-fake-news-a63417.

7 Polyakova A., Boyer S. P., *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, the New Geopolitics, 2018, s. 4, [online:] https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf.

8 MacFarquhar N., *Inside the Russian Troll Factory: Zombies and a Breakneck Pace*, „The New York Times", 2018, [online:] https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html.

9 Richter A., *Disinformation in the media under Russian law*, Europejskie Obserwatorium Audiowizualne, 2019, s. 7, [online:] https://rm.coe.int/disinformation-in-the-media-under-russian-law/1680967369.

10 *Ustawa federalna z dnia 01.05.2019 nr 90-ФЗ o zmianach w ustawie federalnej „W sprawie komunikacji" i ustawie federalnej „W sprawie informacji, technologii informatycznych i ochrony informacji"*, Internetowy portal informacji prawnej, 2019, [online:] http://publication.pravo.gov.ru/Document/View/0001201905010025.

11 Brokeš F., *Russia's sovereign internet*, Obserwator Finansowy, 2019, [online:] https://www.obserwatorfinansowy.pl/in-english/new-trends/russias-sovereign-internet-2-2/.

12 *Rosyjski Kodeks karny* (ang.), 2019, [online:] https://www.imolin.org/doc/amlid/Russian_Federation_Criminal_Code.pdf.

13 *New 'fake news' law stifles independent reporting in Russia on COVID-19*, International Press Institute, 2020, [online:] https://ipi.media/new-fake-news-law-stifles-independent-reporting-in-russia-on-covid-19/.

14 *Примеры публикаций, тиражирующих недостоверную информацию о России*, 2020, [online:] https://www.mid.ru/nedostovernie-publikacii.

15 *Russia to Set Up 'Fake News Database'*, The Moscow Times, 2019, [online:] https://www.themoscowtimes.com/2019/05/16/russia-to-set-up-fake-news-database-a65613.

16 Shaftan V., *Russian Data Localization law: now with monetary penalties*, Norton Rose Fulbright, 2019, [online:] https://www.dataprotectionreport.com/2019/12/russian-data-localization-law-now-with-monetary-penalties/.

17 Miyake K., *China's information warfare is failing again*, The Japan Times, 2020, [online:] https://www.japantimes.co.jp/opinion/2020/03/16/commentary/world-commentary/chinas-information-warfare-failing/.

18 Lyngaas S., *Internal EU report on coronavirus disinformation was harsher on China than public release*, Cyberscoop, [online:] https://www.cyberscoop.com/coronavirus-china-european-union-disinformation/.

19 Jakhar P., *Confucius Institutes: The growth of China's controversial cultural branch*, BBC, 2019, [online:] https://www.bbc.com/news/world-asia-china-49511231.

20 Zhu Z., *Interpreting China's 'Wolf-Warrior Diplomacy'*, The Diplomat, 2020, [online:] https://thediplomat.com/2020/05/interpreting-chinas-wolf-warrior-diplomacy/.

21 *Coronavirus: Chinese official suggests U.S. Army to blame for outbreak*, NBC News, 2020, [online:] https://www.nbcnews.com/news/world/coronavirus-chinese-official-suggests-u-s-army-blame-outbreak-n1157826.

22 EEAS – In detail section, tamże.

23 EEAS report – In detail section, tamże.

24 *Krajowe Biuro Informacji Internetowej wdrożone w celu zwalczania plotek online (oryg.* 国家互联网信息办部署打击网络言*)*, China Daily, 2013, [online:] http://politics.people.com.cn/n/2013/0503/c1001-21348755.html.

25 Tamże.

26 *Translation: Cybersecurity Law of the People's Republic of China*, New America, 2017, [online:] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

27 Wagner J., *China's Cybersecurity Law: What You Need to Know*, The Diplomat, 2017, [online:] https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

28 King G. et al., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, „American Political Science Review" (2017) 111, 3, 2017, s. 488, [online:] https://gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf.

29 Han R., *Defending the Authoritarian Regime Online: China's "Voluntary Fifty-cent Army"*, The China Quarterly, 224, 2015, s. 1009–1010, [online:] https://www.researchgate.net/publication/272490419_Defending_the_Authoritarian_Regime_Online_China's_Voluntary_Fifty-cent_Army.

30 King G. et al., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, op. cit. s. 485.

31 Tamże.

32 Han R., *Defending the Authoritarian Regime Online: China's "Voluntary Fifty-cent Army"*, op. cit.

33 Yang Y., *China's Communist party raises army of nationalist trolls*, Financial Times, 2017, [online:] https://www.ft.com/content/9ef9f592-e2bd-11e7-97e2-916d4fbac0da.

34 *China launches platform to stamp out 'online rumors'*, Reuters, 2018, [online:] https://www.reuters.com/article/us-china-internet/china-launches-platform-to-stamp-out-online-rumors-idUSKCN1LF0HL.

35 Polyakova A., *Weapons of the weak: Russia and AI-driven asymmetric warfare*, Brookings, 2018, [online:] https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

36 Simonite T., *To See the Future of Disinformation, You Build Robo-Trolls*, Wired, 2019, [online:] https://www.wired.com/story/to-see-the-future-of-disinformation-you-build-robo-trolls/.

37 Polyakova A., Boyer S. P., *The Future of Political Warfare*, op. cit., s. 7-10.

38 Alba D., Henkel S., *Russia Tests New Disinformation Tactics in Africa to Expand Influence*, „The New York Times", 2019, [online:] https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html.

39 Stone J., *Chinese accounts blast Trump, with help from AI-generated pictures*, Cyberscoop, 2020, [online:] https://www.cyberscoop.com/graphika-spamouflage-dragon-china/.

40 Vaccari C., Chadwick A., *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, Social Media + Society, 2020, s. 1, [online:] https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408.

41 https://zaodownload.com/

42 https://www.faceapp.com/

43 Gorenburg D., *An Emerging Strategic Partnership: Trends in Russia-China Military Cooperation*, Marshall Center, 2020, [online:] https://www.marshallcenter.org/en/publications/security-insights/emerging-strategic-partnership-trends-russia-china-military-cooperation-0.

44 Stent A., *Russia and China: Axis of revisionists?*, Brookings, 2020, [online:] https://www.brookings.edu/wp-content/uploads/2020/02/FP_202002_russia_china_stent.pdf.

45 *Chinese, Russian diplomats discuss joint efforts against misinformation*, Tass, 2020, [online:] https://tass.com/world/1182301.

46 *Statement by NCSC Director William Evanina: Election Threat Update for the American Public*, NCSC, 2020, [online:] https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

47 Brandt J., Taussig T., *The Kremlin's disinformation playbook goes to Beijing*, Brookings, 2020, [online:] https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.

48 Diresta R., C. Miller, V. Molter, J. Pomfret, G. Tiffert, *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives*, Stanford Internet Observatory, 2020, s. 34, [online:] https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.

49 Opinion: China is overtaking the U.S. as the leader in artificial intelligence, MarketWatch, 2020, [online:] https://www.marketwatch.com/story/china-is-overtaking-the-us-as-the-leader-in-artificial-intelligence-2019-02-27.

50 Cook S., *Welcome to the New Era of Chinese Government Disinformation*, The Diplomat, 2020, [online:] https://thediplomat.com/2020/05/welcome-to-the-new-era-of-chinese-government-disinformation/.

51 Lee K., *Forecasting Synergies in Chinese and Russia Digital Influence Operations*, The Asan Forum, 2020, [online:] http://www.theasanforum.org/forecasting-synergies-in-chinese-and-russia-digital-influence-operations/.

52 Standish R., *China Seen As Rising Military Power In Central Asia, Foreshadowing Future Friction With Russia*, Radio Wolna Europa, 2020, [online:] https://www.rferl.org/a/china-seen-as-rising-military-power-in-central-asia-foreshadowing-future-friction-with-russia/30639964.html.

53 *The Prague Proposals. The Chairman Statement on cyber security of communication networks in a globally digitalized world*, the Prague 5G Security Conference, 2019, [online:] https://www.mzv.cz/file/3481883/PRG_proposals_SP.pdf.

54 *The Clean Network*, US Department of State, 2020, [online]: https://www.state.gov/the-clean-network/.

55 *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, US Department of Justice, 2019, [online:] https://www.justice.gov/storage/report.pdf.

56 Giglietto F., Righetti N., Marino G., *Understanding Coordinated and Inauthentic Link Sharing Behavior on Facebook in the Run-up to 2018 General Election and 2019 European Election in Italy*, LaRiCA - University of Urbino Carlo Bo, 2019, [online:] https://osf.io/preprints/socarxiv/3jteh/.

57 Martens B., Aguiar L., Gomez-Herrera E., Mueller-Langer F., *The digital transformation of news media and the rise of disinformation and fake news*, JRC Digital Economy Working Paper 2018-02, 2018, [online:] https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf.

58 Heatherly Ch. J., Melendez I. A., *Everything Old is New Again: Russian, Chinese, Iranian and North Korean Use of Proxies Against the United States*, Small Wars Journal, 2019, [online:] https://smallwarsjournal.com/jrnl/art/everything-old-new-again-russian-chinese-iranian-and-north-korean-use-proxies-against.

59 *Eeas Special Report Update: Short Assessment Of Narratives And Disinformation Around The Covid-19 Pandemic (Update 23 April – 18 May)*, EEAS, 2020, [online:] https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may/.

60 *Kodeks postępowania w zakresie zwalczania dezinformacji*, Komisja Europejska, 2018, [online:] https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

61 *Tackling online disinformation: Commission proposes an EU-wide Code of Practice*, Komisja Europejska, 2018, [online:] https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3370.

62 *Polska chce podzielić Ukrainę? Żyrinowski: „Dla Ukrainy to i tak za dużo"*, „Newsweek", 2015, [online:] https://www.newsweek.pl/swiat/polska-chce-podzielic-ukrainezyrinowskidla-ukrainy-to-i-tak-za-duzo/blqnr9c.

63 Maciążek P., *Rosja chce zdyskredytować NATO. Fałszywe wywiady polskich generałów*, Defence24, 2016, [online:] https://www.defence24.pl/rosja-chce-zdyskredytowac-nato-falszywe-wywiady-polskich-generalow.

64 Haertle A., *Fałszywy list polskiego generała na stronie www Akademii Sztuki Wojennej*, Zaufana Trzecia Strona, 2020, [online:] https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generala-na-stronie-www-akademii-sztuki-wojennej/.

65 Baran V., *Białoruś. Aleksander Łukaszenka oskarża: „chcą odciąć Grodno, wywiesili tam już polskie flagi"*, Wp.pl, 2020, [online:] https://wiadomosci.wp.pl/bialorus-aleksander-lukaszenka-oskarza-chca-odciac-grodno-wywiesili-tam-juz-polskie-flagi-6545480411495040a.

66 *Disinformation Resilience in Central and Eastern Europe*, Foreign Policy Council "Ukrainian Prism", s. 239, [online:] http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf.

67 *Traktat między Rzeczpospolitą Polską a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej o współpracy w dziedzinie obronności i bezpieczeństwa, sporządzony w Warszawie dnia 21 grudnia 2017 r.*, ISAP Sejm, 2017, [online:] http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190000104.

68 *Secretary Michael R. Pompeo And Polish Foreign Minister Jacek Czaputowicz At a Press Availability*, US Department of State, 2020, [online:] https://www.state.gov/secretary-michael-r-pompeo-and-polish-foreign-minister-jacek-czaputowicz-at-a-press-availability/.

69 *Disinfo: Eastern Partnership And The Three Seas Initiative Are Anti-Russian*, EUvsDisinfo, 2020, [online:] https://euvsdisinfo.eu/report/eastern-partnership-is-a-military-political-anti-russian-flank/.

70 *Disinfo: Three Seas Initiative Is A Geopolitical Concept Designed To Promote American Interests*, EUvsDisinfo, 2019, [online:] https://euvsdisinfo.eu/report/three-seas-initiative-is-a-geopolitical-concept-designed-to-realize-the-american-interests/.

71 Albrycht I. (red), *Bezpieczne cyfrowe DNA Regionu Trójmorza*, Instytut Kościuszki, s. 28–29, 2020, [online:] https://ik.org.pl/wp-content/uploads/raport_bezpieczne_cyfrowe_dna-1.pdf.

72 Czech Startup Wins Tech Challenge To Combat Disinformation, the Horizons Tracker, 2019, [online:] https://adigaskell.org/2019/04/19/czech-startup-wins-tech-challenge-to-combat-disinformation/.

73 Tamże.

74 *Inicjatywa Cyfrowego Trójmorza: Wezwanie Do Nadania Współpracy Regionalnej Silnego Wymiaru Cyfrowego*, Instytut Kościuszki, 2018, [online:] https://www.ik.org.pl/wp-content/uploads/white-paper_inicjatywa_cyfrowego_trojmorza.pdf.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki to wiodący pozarządowy ośrodek naukowo-badawczy o charakterze *non-profit* założony w 2000 r. Naszą misją jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz NATO. Instytut specjalizuje się w tworzeniu strategicznych rekomendacji i kierunków rozwoju kluczowych polityk publicznych, stanowiących merytoryczne wsparcie dla polskich i europejskich decydentów politycznych. Instytut Kościuszki jest pomysłodawcą i głównym organizatorem Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC, corocznej konferencji poświęconej strategicznym aspektom cyberprzestrzeni.

PARTNERZY RAPORTU:

Google

Microsoft

EXATEL

NASK

INSTYTUT KOŚCIUSZKI