



PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIULETYN

Nr 75 (1517), 4 sierpnia 2017 © PISM

Redakcja: Sławomir Dębski ● Bartosz Wiśniewski ● Rafał Tarnogórski
Katarzyna Staniewska (sekretarz redakcji)

Karolina Borońska-Hryniewiecka ● Anna Maria Dynier ● Aleksandra Gawlikowska-Fyk
Sebastian Płóciennik ● Patrycja Sasnal ● Justyna Szczudlik ● Marcin Terlikowski ● Tomasz Żornaczuk

Internet jako narzędzie polityki Chińskiej Republiki Ludowej

Marcin Przychodniak

Władze Chin traktują Internet jako przestrzeń rywalizacji międzynarodowej. Uważają, że wspierany przez UE i USA swobodny dostęp do informacji w globalnej sieci zagraża stabilności ich systemu politycznego. Zacieśniają więc kontrolę Internetu w swoim państwie, dążąc do ograniczenia przepływu informacji. Za element wzmocnienia pozycji ChRL w cyberprzestrzeni uważają także ekspansję gospodarczą chińskich firm z sektora IT za granicą. Inicjują również – konkurencyjny wobec UE i USA – projekt międzynarodowego kodeksu bezpieczeństwa informacyjnego. Działania Chin stoją w sprzeczności z promowaną przez UE otwartością globalnej sieci oraz wolnością gospodarczą.

W październiku 2016 r. wygasła i nie została przedłużona umowa między Departamentem Handlu USA a Internetową Korporacją ds. Nadawania Nazw i Numerów (ICANN), dotycząca zarządzania globalną siecią. Oznaczało to rezygnację Stanów Zjednoczonych z wieloletniego nadzoru nad Internetem, a tym samym konieczność wypracowania przez społeczność międzynarodową nowych zasad administrowania globalną siecią. Równolegle w ONZ toczy się od kilku lat debata na temat zastosowania norm prawa międzynarodowego do Internetu¹. Prace te są związane z cyberprzestępczością, w kontekście zarówno zabezpieczeń przed ewentualnymi atakami, jak i granicy dopuszczalnego odwetu². ChRL bierze udział we wszystkich tych dyskusjach.

Cele Chin w cyberprzestrzeni. Chiny to obecnie państwo z największą na świecie liczbą użytkowników Internetu (730 mln). Działania w cyberprzestrzeni pozwalają władzom ChRL osiągnąć dwa cele: wewnętrzny, czyli kontrolę przepływu informacji w Internecie w celu ochrony reżimu, i zewnętrzny, czyli realizację interesów gospodarczych.

W 2014 r. Komunistyczna Partia Chin (KPCh) powołała Grupę Kierowniczą ds. Bezpieczeństwa Internetowego i Informatyzacji (GKBII). Grupy kierownicze odgrywają kluczową rolę w kształtowaniu polityki Chin, a ich znaczenie wzrosło jeszcze pod rządami Xi Jinpinga. To on kieruje pracami GKBII, a jego zastępcami są inni członkowie Stałego Komitetu Biura Politycznego KPCh: premier Li Keqiang oraz Liu Yunshan – przewodniczący Grupy Kierowniczej ds. Propagandy i Pracy Ideologicznej. Decyzje GKBII realizuje Urząd ds. Cyberprzestrzeni, utworzony w 2014 r. Wykorzystuje do tego m.in. rozbudowę tzw. Great Firewall (systemu blokowania dostępu do serwisów zagranicznych), blokadę VPN (prywatnych sieci umożliwiających obchodzenie blokad treści), biura kontrolerów (na bieżąco usuwających niepożądane treści), a także zmiany legislacyjne (m.in. nakaz lokalizacji serwerów w Chinach, ograniczenia w uruchamianiu serwisów informacyjnych).

Jednocześnie ChRL wspiera ekspansję handlową i inwestycyjną przedsiębiorstw chińskich z sektora IT w Europie Środkowej, Azji Centralnej i Południowo-Wschodniej oraz Afryce. Między innymi dzięki

¹ R. Tarnogórski, *Międzynarodowe zarządzanie i regulacja Internetu*, „Biuletyn PISM”, nr 70 (935), 25 lipca 2012 r.

² R. Tarnogórski, *Prawo konfliktów zbrojnych a cyberprzestrzeń*, „Biuletyn PISM”, nr 31 (1007), 26 marca 2013 r.

zamknięciu chińskiego rynku dla zagranicznej konkurencji i pomocy finansowej przedsiębiorstwa takie jak Alibaba, Huawei czy Lenovo zyskały status marek globalnych. Firmy te aktywnie włączyły się w inicjatywę Pasa i Szlaku (BRI), której elementem jest budowa połączeń telekomunikacyjnych. W Europie Środkowej powstały biura regionalne chińskich koncernów Huawei (Warszawa) i ZTE (Budapeszt). Huawei – oprócz rozbudowy w Polsce infrastruktury sieciowej na potrzeby telefonii komórkowej – zajmuje także drugą pozycję pod względem udziałów na polskim rynku smartfonów. Strategia chińskiego Ministerstwa Przemysłu i Technologii Informatycznej z 2016 r. zakłada zainwestowanie ponad 170 mld dol. w budowę i modernizację sieci telekomunikacyjnych w Afryce w ciągu kolejnych dwóch lat. Huawei i ZTE łącznie założyły centra szkoleniowe w 9 państwach afrykańskich, a w ponad 20 innych zbudowały infrastrukturę sieciową. Także firmy z sektora e-commerce (np. Alibaba i JD.com) budują 20 magazynów w krajach objętych BRI (np. Indonezji). Alibaba stworzyła specjalną cyfrową strefę wolnego handlu w Malezji.

Chiny regulują również swoje relacje z innymi krajami w zakresie cyberbezpieczeństwa. Chcą w ten sposób zmienić wizerunek państwa oskarżanego o wspieranie szpiegostwa przemysłowego i kradzieży własności intelektualnej z wykorzystaniem Internetu. W 2015 r. ChRL podpisała umowę z USA, w której obie strony wyrzekły się podobnych praktyk. Nie wyeliminowało to całkowicie tego procederu, ale spadła liczba takich ataków ze strony Chin. Podobne porozumienia chińskie władze zawarły z Wielką Brytanią i Kanadą. Szczególny charakter ma umowa z Rosją z 2015 r. Zawarta jest w niej klauzula o wzajemnej „nieagresji” w cyberprzestrzeni, chociaż ma ona znaczenie bardziej polityczne niż praktyczne. Chiny są bowiem świadome zagrożenia ze strony Rosji, a w raporcie firmy internetowej Qihoo 360 z 2017 r. wskazano, że wśród aktywnie działających w ChRL grup hakerskich są także podmioty rosyjskie.

Chiny wobec zarządzania Internetem. Władze chińskie podkreślają, że nie do przyjęcia jest obecna sytuacja, w której światowa sieć podlega normom narzuconym wcześniej przez USA. ChRL wielokrotnie zaznaczała, że 10 z 13 głównych serwerów DNS przechowujących informacje na temat podstawowych adresów internetowych znajduje się w Stanach Zjednoczonych. Po wygaśnięciu umowy między USA a ICANN Chiny zgłosiły postulat przyznania państwom rozwijającym się większej roli w tej organizacji.

ChRL promuje koncepcję „suwerennościową”. Sankcjonuje ona prawo państw do kontroli przepływu treści w Internecie czy wyboru modelu zarządzania siecią. Odmienne stanowisko reprezentuje UE, dla której Internet jest platformą otwartą dla wszystkich. Podejście USA było dotąd zbieżne z unijnym. Może jednak ulec modyfikacji, na co wskazuje m.in. fakt, że z ostatecznej wersji rozporządzenia wykonawczego prezydenta USA w sprawie cyberbezpieczeństwa, opublikowanej w maju br., usunięto fragment o wsparciu wielostronnego modelu zarządzania Internetem.

W debacie na temat cyberprzestrzeni Chiny, inaczej niż USA i UE, podkreślają, że istniejące normy prawne nie przystają do Internetu i konieczne jest opracowanie nowych regulacji. Dlatego w 2015 r. (z udziałem Szanghajskiej Organizacji Współpracy) zgłosiły do ZO ONZ zaktualizowany projekt międzynarodowego kodeksu bezpieczeństwa informacyjnego. Przewiduje on rozwiązania wzmacniające rolę państw w ramach zarządzania Internetem, ale jest na tyle kontrowersyjny, że debata nad nim się opóźnia. Chiny uważają ONZ za właściwe forum prac nad regulacjami w zakresie cyberprzestrzeni. Dlatego nie zdecydowały się przystąpić do Konwencji Rady Europy o cyberprzestępczości z 2001 r. – uznały ją za zbyt europocentryczną i nieuwzględniającą postulatów koncepcji „suwerennościowej”. Aktywnie uczestniczyły za to w pracach Grupy Ekspertów Rządowych ds. Rozwoju Informatyki i Telekomunikacji w kontekście Bezpieczeństwa Międzynarodowego w ramach ONZ. Grupa ta miała określić, w jakim stopniu prawo międzynarodowe odnosi się do Internetu. Nie udało się jednak osiągnąć kompromisu, a jednym z powodów była postawa Chin, które np. odrzuciły (m.in. wraz z Rosją, Białorusią czy Malezją) stanowisko w sprawie zastosowania prawa do samoobrony (art. 51 Karty NZ) do ataków w cyberprzestrzeni.

Wnioski. Chiny nie zrezygnują z promowania koncepcji „suwerennościowej”, gdyż jest ona kluczowa dla stabilizacji reżimu. Ponadto dzięki niej mogą występować jako lider koalicji państw sprzeciwiających się obecnym rozwiązaniom. Proponowane przez ChRL wzmocnienie roli państw w zarządzaniu Internetem może się przełożyć na ograniczenie przepływu informacji i rozwoju technologii internetowych. Niezbędne jest więc podtrzymanie unijnego sprzeciwu wobec tych koncepcji na forach międzynarodowych, zwłaszcza wobec możliwej modyfikacji stanowiska USA.

W Polsce i innych państwach Europy Środkowej obecność chińskich podmiotów wiąże się z wymiernymi korzyściami, np. w zakresie inwestycji w infrastrukturę, z czego korzysta branża teleinformatyczna. Z ostrożnością należy jednak podchodzić do inicjatyw politycznych związanych z cyberprzestrzenią, które zmierzałyby do umocnienia koncepcji „suwerennościowej”. Debata na temat prawnych aspektów funkcjonowania Internetu na forum ONZ będzie kontynuowana w 2018 r., czyli w okresie polskiego członkostwa w RB ONZ. Dla Polski korzystniejsze jest wsparcie otwartego modelu zarządzania siecią, sprzyjającego rozwojowi sektora nowych technologii i branży internetowej.